kaspersky

Kaspersky Endpoint Security pro systém Windows 11.6.0

Obsah

Často kladené dotazy

OBECNÉ

Na jakých počítačích může aplikace Kaspersky Endpoint Security fungovat?

Co se změnilo od poslední verze?

Se kterými dalšími aplikacemi společnosti Kaspersky může aplikace Kaspersky Endpoint Security fungovat?

Jak lze šetřit počítačové prostředky během provozu aplikace Kaspersky Endpoint Security?

NASAZENÍ

Jak nainstaluji aplikaci Kaspersky Endpoint Security do všech počítačů v organizaci?

Které nastavení instalace lze konfigurovat v příkazovém řádku?

Jak mohu vzdáleně odinstalovat aplikaci Kaspersky Endpoint Security?

AKTUALIZACE

Jaké metody jsou k dispozici pro aktualizaci databází?

Co mám dělat, pokud vzniknou problémy po aktualizaci?

Jak mohu aktualizovat databáze mimo podnikovou síť?

Je možné pro aktualizace použít proxy server?

BEZPEČNOST

Jak aplikace Kaspersky Endpoint Security kontroluje e-mail?

Jak mohu vyloučit důvěryhodný soubor z kontroly?

Jak mohu chránit počítač před viry z flash disků?

Jak mohu spustit antivirovou kontrolu, která je skrytá před uživatelem?

Jak dočasně pozastavit ochranu aplikace Kaspersky Endpoint Security?

Jak mohu obnovit soubor, který aplikace Kaspersky Endpoint Security chybně odstranila?

Jak mohu chránit aplikaci Kaspersky Endpoint Security před odinstalováním uživatelem?

INTERNET

Prohledává aplikace Kaspersky Endpoint Security šifrovaná připojení (HTTPS)?

Jak mohu uživatelům povolit připojení pouze k důvěryhodným sítím Wi-Fi?

Jak zablokovat sociální sítě?

APLIKACE

Jak zjistím, které aplikace jsou nainstalovány v počítači uživatele (inventarizace)?

Jak zabráním spouštění počítačových her?

Jak ověřím, že byla správně nakonfigurována součást Kontrola aplikací?

Jak přidám aplikaci na seznam důvěryhodných aplikací?

ZAŘÍZENÍ

Jak zablokovat použití flash disků?

Jak přidám zařízení na seznam důvěryhodných zařízení?

Je možné získat přístup k blokovanému zařízení?

ŠIFROVÁNÍ

Za jakých podmínek je šifrování nemožné?

Jak mohu použít heslo k omezení přístupu k archivu?

Je možné používat čipové karty a tokeny se šifrováním?

Je možné získat přístup k šifrovaným datům, když není navázáno s aplikací Kaspersky Security Center?

Co mám dělat, pokud operační systém počítače selže, ale data zůstanou zašifrovaná?

PODPORA

Kde je uložen soubor zprávy?

Jak mohu vytvořit trasovací soubor?

Jak mohu povolit zápis výpisu paměti?

Co je nového

Aktualizace 11.6.0

Aplikace Kaspersky Endpoint Security 11.6.0 pro systém Windows nabízí následující funkce a vylepšení:

1. Podpora pro Windows 10 21H1. Podrobnosti o podpoře operačního systému Microsoft Windows 10 najdete ve znalostní bázi technické podpory.

2. Byla přidána součást Managed Detection and Response. Tato součást umožňuje interakci s řešením známým jako Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* poskytuje nepřetržitou ochranu před rostoucím počtem hrozeb schopných obejít automatizované ochranné mechanismy pro organizace, které obtížně hledají vysoce kvalifikované odborníky nebo mají omezené interní zdroje. Podrobné informace o tom, jak řešení funguje, *najdete v průvodci nápovědou k aplikaci Kaspersky Managed Detection and Response*.

3. Aplikace Kaspersky Endpoint Agent, který je součástí distribuční sady, byla aktualizována na verzi 3.10. Kaspersky Endpoint Agent 3.10 poskytuje nové funkce, řeší některé předchozí problémy a má vylepšenou stabilitu. Další podrobnosti o aplikaci najdete v dokumentaci řešení Kaspersky, která podporují aplikaci Kaspersky Endpoint Agent.

4. Nově poskytuje možnost spravovat v nastavení součásti Ochrana před síťovými hrozbami ochranu před útoky, jako jsou přehlcení sítě nebo skenování portů.

5. Byla přidána nová metoda vytváření pravidel sítě pro bránu firewall. Můžete přidat pravidla paketů a pravidla aplikací pro připojení, která se zobrazují v okně Sledování sítě. Nastavení připojení pravidel sítě se však nakonfigurují automaticky.

6. Bylo vylepšeno rozhraní Sledování sítě. Byly přidány informace o síťové aktivitě: ID procesu, který iniciuje síťovou aktivitu; typ sítě (místní síť nebo internet); místní porty. Ve výchozím nastavení jsou informace o typu sítě skryté.

7. Nově existuje možnost automaticky vytvářet účty ověřovacího agenta pro nové uživatele systému Windows. Agent umožňuje uživateli provést ověření pro přístup k jednotkám, které byly šifrovány pomocí technologie Kaspersky Disk Encryption, a načíst operační systém. Aplikace kontroluje informace o uživatelských účtech systému Windows v počítači. Pokud aplikace Kaspersky Endpoint Security zjistí uživatelský účet systému Windows, který nemá účet ověřovacího agenta, aplikace vytvoří nový účet pro přístup k šifrovaným jednotkám. To znamená, že u počítačů s již zašifrovanými jednotkami nemusíte ručně přidávat účty ověřovacího agenta.

8. Nově existuje možnost sledovat proces šifrování disku v rozhraní aplikace na počítačích uživatelů (Kaspersky Disk Encryption a BitLocker). Nástroj Sledování šifrování můžete spustit z hlavního okna aplikace.

Aktualizace 11.5.0

Aplikace Kaspersky Endpoint Security 11.6.0 pro systém Windows nabízí následující funkce a vylepšení:

1. Podpora pro Windows 10 20H2. Podrobnosti o podpoře operačního systému Microsoft Windows 10 najdete ve znalostní bázi technické podpory.

2. Aktualizované rozhraní aplikace. Aktualizována byla také ikona aplikace v oznamovací oblasti, oznámení aplikace a dialogová okna.

3. Vylepšené rozhraní webového pluginu Kaspersky Endpoint Security pro součásti Kontrola aplikací, Kontrola zařízení a Adaptivní kontrola anomálií.

4. Přidána funkce pro import a export seznamů pravidel a výjimek ve formátu XML. Formát XML umožňuje seznamy po jejich exportu upravovat. Seznamy můžete spravovat ve webové konzole aplikace Kaspersky Security Center. Pro export/import jsou k dispozici následující seznamy:

   - Detekce chování (seznam výjimek).
   - Ochrana před webovými hrozbami (seznam důvěryhodných webových adres).
   - Ochrana před hrozbami v poště (seznam přípon filtrů příloh).
   - Ochrana před síťovými hrozbami (seznam výjimek).
   - Brána firewall (seznam pravidel síťových paketů).
   - Kontrola aplikací (seznam pravidel).
   - Kontrola webu (seznam pravidel).
   - Monitorování síťových portů (seznamy portů a aplikací monitorovaných aplikací Kaspersky Endpoint Security).
   - Kaspersky Disk Encryption (seznam výjimek).
   - Šifrování vyměnitelných jednotek (seznam pravidel).

5. Do zprávy o detekci hrozeb byly přidány informace o objektu MD5. V předchozích verzích aplikace Kaspersky Endpoint Security se zobrazovala pouze hodnota SHA256 objektu.

6. Přidána možnost přiřadit prioritu pravidlům pro přístup k zařízením v nastavení součásti Kontrola zařízení. Prioritní přiřazení umožňuje flexibilnější konfiguraci přístupu uživatelů k zařízením. Pokud byl uživatel přidán do více skupin, řídí aplikace Kaspersky Endpoint Security přístup k zařízení na základě pravidla s nejvyšší prioritou. Například můžete skupině Všichni udělit oprávnění jen pro čtení a skupině správců udělit oprávnění ke čtení a zápisu. Chcete-li tak učinit, přiřaďte skupině správců prioritu 0 a skupině Všichni prioritu 1. Prioritu můžete nakonfigurovat pouze pro zařízení, která mají souborový systém. To zahrnuje pevné disky, vyměnitelné jednotky, diskety, jednotky CD/DVD a přenosná zařízení (MTP).

7. Přidána nová funkce:

   - Správa zvukových oznámení.
   - Funkce aplikace Kaspersky Endpoint Security Provoz sítě s ohledem na náklady omezuje vlastní síťový provoz, pokud je omezeno připojení k internetu (například při mobilním připojení).
   - Nastavení aplikace Kaspersky Endpoint Security lze spravovat pomocí důvěryhodných aplikací pro vzdálenou správu (např. TeamViewer, LogMeIn a Remotely Anywhere). Ke spuštění aplikace Kaspersky Endpoint Security a ke správě nastavení v rozhraní aplikace můžete použít aplikace vzdálené správy.
   - Nastavení kontroly bezpečného provozu lze spravovat ve Firefoxu a Thunderbirdu. Můžete vybrat úložiště certifikátů, které bude používat Mozilla: úložiště certifikátů Windows, nebo úložiště certifikátů Mozilly. Tato funkce je k dispozici pouze pro počítače, na nichž se nepoužívá zásada. Pokud se na počítač používá zásada zásady, aplikace Kaspersky Endpoint Security automaticky povolí použití úložiště certifikátů Windows ve Firefoxu a Thunderbirdu.

8. Přidána možnost konfigurace režimu kontroly bezpečného provozu: lze kontrolovat provoz vždy, i když jsou součásti ochrany deaktivovány, nebo pokud to vyžadují součásti ochrany.

9. Revidován postup pro odstraňování informací ze zpráv. Uživatel může odstranit pouze všechny zprávy. V předchozích verzích aplikace si uživatel mohl vybrat konkrétní součásti aplikace, jejichž informace by byly odstraněny ze zpráv.

10. Revidován postup pro import konfiguračního souboru obsahujícího nastavení aplikace Kaspersky Endpoint Security a revidován postup pro obnovení nastavení aplikace. Před importem nebo obnovením zobrazí aplikace Kaspersky Endpoint Security pouze varování. V předchozích verzích aplikace bylo možné zobrazit hodnoty nového nastavení před jejich použitím.

11. Zjednodušen postup pro obnovení přístupu k jednotce, která byla šifrována nástrojem BitLocker. Po dokončení postupu pro obnovení přístupu vyzve aplikace Kaspersky Endpoint Security uživatele k nastavení nového hesla nebo PIN kódu. Po nastavení nového hesla BitLocker zašifruje disk. V předchozí verzi aplikace musel uživatel ručně resetovat heslo v nastavení nástroje BitLocker.

12. Uživatelé nyní mají schopnost vytvořit vlastní místní důvěryhodnou zónu pro konkrétní počítač. Tímto způsobem mohou uživatelé kromě obecné důvěryhodné zóny v zásadách vytvářet také vlastní místní seznamy výjimek a důvěryhodných aplikací. Správce může povolit nebo zablokovat použití místních výjimek nebo místních důvěryhodných aplikací. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

13. Přidána možnost zadávat komentáře ve vlastnostech důvěryhodných aplikací. Komentáře pomáhají zjednodušit vyhledávání a řazení důvěryhodných aplikací.

14. Správa aplikace prostřednictvím rozhraní REST API:

    - Nyní existuje možnost konfigurovat nastavení rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook.
    - Je zakázáno deaktivovat detekci virů, červů a trojských koní.

Aktualizace 11.4.0

Aplikace Kaspersky Endpoint Security 11.4.0 pro systém Windows nabízí následující funkce a vylepšení:

1. Nový design ikony aplikace v oznamovací oblasti hlavního panelu. Místo staré ikony se nyní zobrazuje nová . Pokud má uživatel provést akci (například restartovat počítač po aktualizaci aplikace), ikona se změní na . Pokud jsou součásti ochrany aplikace deaktivovány nebo jsou nefunkční, ikona se změní na nebo . Když umístíte kurzor myši na ikonu, aplikace Kaspersky Endpoint Security zobrazí popis problému s ochranou počítače.

2. Součást Kaspersky Endpoint Agent, který je součástí distribuční sady, byla aktualizována na verzi 3.9. Kaspersky Endpoint Agent 3.9 podporuje integraci s novými řešeními společnosti Kaspersky. Další podrobnosti o aplikaci najdete v dokumentaci řešení Kaspersky, která podporují aplikaci Kaspersky Endpoint Agent.

3. Byl přidán stav *Nepodporováno licencí* pro součásti aplikace Kaspersky Endpoint Security. Stav součástí si můžete prohlédnout kliknutím na tlačítko **Součásti ochrany** v hlavním okně aplikace.

4. Do zpráv byly přidány nové události ze součásti Prevence zneužití.

5. Ovladače pro technologii Kaspersky Disk Encryption se po spuštění šifrování disku nyní automaticky přidají do prostředí Windows Recovery Environment (WinRE). Při instalaci aplikace přidávala předchozí verze aplikace Kaspersky Endpoint Security ovladače. Přidání ovladačů do prostředí WinRE může zlepšit stabilitu aplikace při obnově operačního systému v počítačích chráněných technologií Kaspersky Disk Encryption.

Z aplikace Kaspersky Endpoint Security byla odebrána součást Endpoint Sensor. Nastavení součást Endpoint Sensor můžete i nadále konfigurovat v zásadách, je-li v počítači nainstalována aplikace Kaspersky Endpoint Security verze 11.0.0 až 11.3.0.

Kaspersky Endpoint Security pro systém Windows

Aplikace Kaspersky Endpoint Security pro systém Windows (dále označována také jako Kaspersky Endpoint Security) poskytuje komplexní ochranu počítače před různými typy hrozeb, síťových a phishingových útoků.

Pro ochranu vašeho počítače Kaspersky Endpoint Security používá následující technologie zjišťování hrozeb:

- **Strojové učení**. Kaspersky Endpoint Security používá model založený na strojovém učení. Tento model byl vyvinut odborníky společnosti Kaspersky. Během používání model neustále dostává aktualizované údaje o hrozbách ze služby KSN, čímž se trénuje.

- **Analýza cloudu**. Kaspersky Endpoint Security dostává ze služby Kaspersky Security Network údaje o hrozbách. *Služba Kaspersky Security Network (KSN)* představuje infrastrukturu cloudových služeb, která poskytuje přístup k internetové znalostní bázi společnosti Kaspersky s informacemi o reputaci souborů, webových prostředcích a softwaru.

- **Odborná analýza**. Kaspersky Endpoint Security používá údaje o hrozbách přidávané analytiky virů společnosti Kaspersky. Pokud nelze reputaci objektu určit automaticky, analytikové virů jej kontrolují ručně.

- **Analýza chování**. Kaspersky Endpoint Security analyzuje aktivitu objektu v reálném čase.

- **Automatická analýza**. Kaspersky Endpoint Security dostává data ze systému automatické analýzy objektů. Systém zpracovává všechny objekty přijaté společností Kaspersky a poté určí jejich reputaci a přidá do antivirové databáze příslušné údaje. Pokud systém nedokáže určit reputaci objektu, odešle požadavek virovým analytikům společnosti Kaspersky.

- **Kaspersky Sandbox**. Kaspersky Endpoint Security kontroluje objekty ve virtuálním počítači. Kaspersky Sandbox analyzuje chování objektu a rozhodne o jeho reputaci. Tato technologie je k dispozici, pouze pokud používáte Kaspersky Sandbox.

Každý typ hrozby je zpracováván vyhrazenou součástí. Součásti lze povolovat a zakazovat nezávisle a lze konfigurovat jejich nastavení.

Následující součásti aplikace jsou součásti kontroly:

- **Kontrola aplikací**. Tato součást umožňuje sledovat pokusy uživatelů o spuštění aplikací a reguluje spouštění aplikací.

- **Kontrola zařízení**. Tato součást umožňuje konfigurovat flexibilní omezení přístupu k zařízením pro ukládání dat (např. pevné disky, vyměnitelné jednotky a disky CD/DVD), zařízením pro přenos dat (např. modemy), zařízením pro převod informací (např. tiskárny) nebo rozhraním pro připojení zařízení k počítačům (např. USB, Bluetooth).

- **Kontrola webu**. Tato součást umožňuje nastavit flexibilní omezení přístupu k webovým prostředkům pro různé skupiny uživatelů.

- **Adaptivní kontrola anomálií**. Tato součást sleduje a reguluje potenciálně škodlivé akce, které nejsou obvyklé pro chráněný počítač.

Následující součásti aplikace jsou součásti ochrany:

- **Detekce chování**. Tato součást přijímá informace o akcích aplikací v počítači a tyto informace poskytuje jiným součástem, což zvyšuje účinnost ochrany.

- **Prevence zneužití**. Tato součást sleduje spustitelné soubory, které jsou spouštěny zranitelnými aplikacemi. Pokud dojde k pokusu o spuštění spustitelného souboru ze zranitelné aplikace, který neučinil uživatel, aplikace Kaspersky Endpoint Security spuštění tohoto souboru zablokuje.

- **Prevence narušení hostitele**. Tato součást registruje akce aplikací v operačním systému a reguluje činnosti aplikací v závislosti na skupině důvěryhodnosti určité aplikace. Pro každou skupinu aplikací je definována sada pravidel. Tato pravidla regulují přístup aplikací k uživatelským datům a prostředkům operačního systému. Mezi tato data patří uživatelské soubory ve složce Dokumenty, soubory cookie, soubory protokolů činnosti uživatelů a soubory, složky a klíče registru, které obsahují nastavení a důležité informace z nejčastěji používaných aplikací.

- **Modul pro nápravu**. Tato součást umožňuje aplikaci Kaspersky Endpoint Security vrátit zpět akce, které byly provedeny malwarem v operačním systému.

- **Ochrana před souborovými hrozbami**. Tato součást chrání souborový systém počítače před infekcí. Součást se spustí ihned po spuštění aplikace Kaspersky Endpoint Security. Trvale zůstává v paměti RAM počítače a kontroluje všechny otevírané, ukládané a spouštěné soubory v počítači a všech připojených paměťových zařízeních. Tato součást zachytí každý pokus o přístup k souboru a soubor zkontroluje na přítomnost virů a jiných hrozeb.

- **Ochrana před webovými hrozbami**. Tato součást kontroluje provoz směřující do počítače uživatele přes protokoly HTTP a FTP a kontroluje, zda nejsou webové adresy škodlivé nebo zda neobsahují phishing.

- **Ochrana před hrozbami v poště**. Tato součást kontroluje příchozí a odchozí e-maily na přítomnost virů a jiných hrozeb.

- **Ochrana před síťovými hrozbami**. Tato součást kontroluje příchozí síťový provoz, který je obvyklý pro síťové útoky. Pokud aplikace Kaspersky Endpoint Security zjistí pokus o síťový útok na počítač, zablokuje síťovou komunikaci ze strany útočícího počítače.

- **Brána firewall**. Tato součást chrání data uložená v počítači a blokuje většinu možných hrozeb pro operační systém, když je počítač připojený k internetu nebo místní síti.

- **Ochrana před útoky BadUSB**. Tato součást brání tomu, aby se infikovaná zařízení USB napodobující klávesnici připojila k počítači.

- **Ochrana AMSI**. Tato součást kontroluje objekty na základě požadavku od aplikací třetích stran a žádající aplikaci oznámí výsledek kontroly.

Kromě ochrany v reálném čase zajišťované součástmi aplikace doporučujeme provádět pravidelnou *kontrolu počítače* na přítomnost virů a jiných hrozeb. Pomůže to vyloučit možnost šíření malwaru, který nebyl zjištěn součástmi ochrany, například v důsledku nízké úrovně zabezpečení.

Aby byla ochrana počítače aktuální, je nutné *aktualizovat databáze a moduly*, které aplikace používá. Aplikace je ve výchozím nastavení aktualizována automaticky. V případě potřeby však můžete aktualizovat databáze a moduly aplikace ručně.

Aplikace Kaspersky Endpoint Security poskytuje tyto úlohy:

- **Kontrola integrity**. Aplikace Kaspersky Endpoint Security zkontroluje moduly aplikace v instalační složce aplikace z hlediska změn nebo poškození. Pokud má modul aplikace nesprávný digitální podpis, je považován za poškozený.

- **Úplná kontrola**. Aplikace Kaspersky Endpoint Security kontroluje operační systém, včetně paměti jádra, objektů načítaných při spouštění operačního systému, spouštěcích sektorů disků, úložiště zálohy operačního systému a všech pevných disků a vyměnitelných jednotek.

- **Uživatelská kontrola**. Aplikace Kaspersky Endpoint Security kontroluje objekty, které vybral uživatel.

- **Kontrola kritických oblastí**. Aplikace Kaspersky Endpoint Security kontroluje paměť jádra, objekty načítané při spouštění operačního systému a spouštěcí sektory disků.

- **Aktualizace**. Aplikace Kaspersky Endpoint Security stahuje aktualizované databáze a moduly aplikace. Aktualizace chrání počítač před nejnovějšími viry a jinými hrozbami.

- **Vrácení změn provedených poslední aktualizací**. Aplikace Kaspersky Endpoint Security vrátí zpět poslední aktualizaci databází a modulů. To v případě potřeby umožňuje vrátit zpět moduly databází a aplikací na jejich předchozí verze, například když nová verze databáze obsahuje neplatný podpis, který způsobí, že aplikace Kaspersky Endpoint Security zablokuje bezpečnou aplikaci.

Funkce služeb aplikace

Aplikace Kaspersky Endpoint Security zahrnuje řadu funkcí služeb. Účelem poskytování funkcí služeb je udržování aplikace v aktuálním stavu, rozšiřování jejích funkcí a poskytování pomoci uživatelům s použitím aplikace.

- **Zprávy**. Aplikace během provozu uchovává zprávu o každé součásti aplikace. Zprávy můžete také použít ke sledování výsledků dokončených úloh. Zprávy obsahují seznamy událostí, které se vyskytly během činnosti aplikace Kaspersky Endpoint Security, a všech operací prováděných aplikací. Když dojde k incidentu, můžete odeslat zprávy společnosti Kaspersky. Její odborníci technické podpory mohou následně váš problém podrobněji prozkoumat.

- **Úložiště dat**. Jestliže aplikace při kontrole počítače na přítomnost virů a jiných hrozeb zjistí infikované soubory, tyto soubory zablokuje. Aplikace Kaspersky Endpoint Security ukládá kopie dezinfikovaných a odstraněných souborů v modulu *Záloha*. Aplikace Kaspersky Endpoint Security přesune soubory, které nejsou z nějakého důvodu zpracovány, na *seznam aktivních hrozeb*. Můžete kontrolovat soubory, obnovit je v původních složkách a také můžete vyprázdnit úložiště dat.

- **Oznamovací služba**. Oznamovací služba pomáhá uživateli sledovat události, které ovlivňují stav ochrany počítače a činnost aplikace Kaspersky Endpoint Security. Upozornění mohou být zobrazena na obrazovce nebo odeslána e-mailem.

- **Kaspersky Security Network**. Účast uživatelů v rámci služby Kaspersky Security Network zvyšuje účinnost ochrany počítače tím, že v reálném čase používá informace o reputaci souborů, webových prostředků a softwaru přijatých od uživatelů z celého světa.

- **Licence**. Nákup licence odemkne všechny funkce aplikace, poskytne přístup k aktualizacím databáze a modulů aplikace a umožní využívat telefonní nebo e-mailovou podporu, která pomáhá s řešením potíží s instalací, konfigurací a použitím aplikace.

- **Podpora**. Všichni registrovaní uživatelé aplikace Kaspersky Endpoint Security mohou kontaktovat odborníky technické kontroly a požádat je o pomoc. Požadavek technické podpoře společnosti Kaspersky můžete odeslat prostřednictvím portálu Kaspersky CompanyAccount nebo se můžete s technickou podporou spojit telefonicky.

Pokud aplikace vrátí chyby nebo se najednou zablokuje, může být automaticky restartována.

Jestliže aplikace zjistí opakované chyby, které způsobují zhroucení aplikace, aplikace provede následující akce:

1. Zakáže funkce kontroly a ochrany (funkce šifrování zůstane povolena).

2. Upozorní uživatele na to, že byly dané funkce zakázány.

3. Po aktualizaci antivirových databází nebo modulů aplikace se pokusí obnovit funkční stav aplikace.

Distribuční sada

Distribuční sada obsahuje následující distribuční balíčky:

- **Silné šifrování (AES256)**

  Tento distribuční balíček obsahuje šifrovací nástroje, které implementují šifrovací algoritmus AES (Advanced Encryption Standard) s účinnou délkou klíče 256 bitů.

- **Lehké šifrování (AES56)**

  Tento distribuční balíček obsahuje šifrovací nástroje, které implementují šifrovací algoritmus AES s účinnou délkou klíče 56 bitů.

Každý šifrovací balíček obsahuje následující soubory:

`kes_win.msi`	Instalační balíček aplikace Kaspersky Endpoint Security.
`setup_kes.exe`	Soubory, které jsou třeba k instalaci aplikace za použití kteréhokoli z dostupných způsobů.
`kes_win.kud`	Soubor k vytvoření instalačních balíčků aplikace Kaspersky Endpoint Security.
`klcfginst.msi`	Instalační balíček modulu plug-in pro správu aplikace Kaspersky Endpoint Security pro aplikaci Kaspersky Security Center.
`bases.cab`	Soubory aktualizačního balíčku používané během instalace.
`cleaner.cab`	Soubory k odebrání nekompatibilního softwaru.
`incompatible.txt`	Soubor, který obsahuje seznam nekompatibilního softwaru.
`ksn_<ID_jazyka>.txt`	Soubor, ve kterém si můžete projít podmínky účasti ve službě Kaspersky Security Network.
`license.txt`	Soubor, ve kterém si můžete projít licenční smlouvu s koncovým uživatelem a zásady ochrany osobních údajů.
`installer.ini`	Soubor, který obsahuje vnitřní nastavení distribučního balíčku.
`endpointagent.msi`	Instalační balíček aplikace Kaspersky Endpoint Agent verze 3.10, což je aplikace vyžadovaná pro integraci s dalšími řešeními společnosti Kaspersky (například Kaspersky Sandbox).
`NDP<verze>-<vlastnosti balíčku>`	Instalační balíček rozhraní Microsoft .NET Framework.
`keswin_web_plugin.zip`	Archiv obsahující soubory potřebné k instalaci webového pluginu Kaspersky Endpoint Security.

Hodnoty těchto nastavení nedoporučujeme měnit. Pokud chcete změnit možnosti instalace, použijte soubor setup.ini.

Hardwarové a softwarové požadavky

Aby aplikace Kaspersky Endpoint Security mohla bez problémů fungovat, počítač musí splňovat následující požadavky:

Minimální obecné požadavky:

- 2 GB volného místa na pevném disku
- CPU:
  - Pracovní stanice: 1 GHz
  - Server: 1,4 GHz
  - Podpora sady instrukcí SSE2
- RAM:
  - Pracovní stanice (x86): 1 GB
  - Pracovní stanice (x64): 2 GB
  - Server: 2 GB
- Microsoft .NET Framework 4.0 nebo novější

Podporované operační systémy pro pracovní stanice:

- Windows 7 Home/Professional/Ultimate/Enterprise Service Pack 1 nebo novější;
- Windows 8 Professional/Enterprise;
- Windows 8.1 Professional/Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise.

Algoritmus podpisu modulu SHA-1 přestává společnost Microsoft používat. Pro úspěšnou instalaci aplikace Kaspersky Endpoint Security do počítače s operačním systémem Microsoft Windows 7 je nutná aktualizace KB4474419. Další informace o této aktualizaci naleznete na webu technické podpory společnosti Microsoft.

Podrobnosti o podpoře operačního systému Microsoft Windows 10 najdete ve znalostní bázi technické podpory.

Podporované operační systémy pro servery:

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

  Microsoft Small Business Server 2011 Standard (64bitová verze) je podporován pouze v případě, že je nainstalována aktualizace Service Pack 1 pro Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64bitová verze)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 nebo novější;
- 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.

Algoritmus podpisu modulu SHA-1 přestává společnost Microsoft používat. Pro úspěšnou instalaci aplikace Kaspersky Endpoint Security do počítače s operačním systémem Microsoft Windows Server 2008 R2 je nutná aktualizace KB4474419. Další informace o této aktualizaci naleznete na webu technické podpory společnosti Microsoft.

Podrobnosti o podpoře operačních systémů Microsoft Windows Server 2016 a Microsoft Windows Server 2019 najdete ve znalostní bázi technické podpory.

Podporované typy terminálového serveru:

- Microsoft Remote Desktop Services na základě Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services na základě Windows Server 2012;
- Microsoft Remote Desktop Services na základě Windows Server 2012 R2;
- Microsoft Remote Desktop Services na základě Windows Server 2016;
- Microsoft Remote Desktop Services na základě Windows Server 2019.

Podporované virtuální platformy:

- VMWare Workstation 16 Pro
- Aktualizace VMware ESXi 7.0 1a
- Microsoft Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Kaspersky Endpoint Security funguje s následujícími verzemi aplikace Kaspersky Security Center:

- Kaspersky Security Center 11
- Kaspersky Security Center 12
- Kaspersky Security Center 12 s bezpečnostní opravou A
- Kaspersky Security Center 12 s bezpečnostní opravou B
- Kaspersky Security Center 12
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2

Porovnání dostupných funkcí aplikace v závislosti na typu operačního systému

Sada dostupných funkcí aplikace Kaspersky Endpoint Security závisí na typu operačního systému: pracovní stanice, nebo server (viz tabulka níže).

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Pracovní stanice	Server
Rozšířená ochrana před hrozbami		
Služba hodnocení reputace KSN	✓	✓
Detekce chování	✓	✓
Prevence zneužití	✓	✓
Prevence narušení hostitele	✓	–
Modul pro nápravu	✓	✓
Základní ochrana před hrozbami		
Ochrana před souborovými hrozbami	✓	✓
Ochrana před webovými hrozbami	✓	–
Ochrana před hrozbami v poště	✓	–
Brána firewall	✓	✓
Ochrana před síťovými hrozbami	✓	✓
Ochrana před útoky BadUSB	✓	✓
Ochrana AMSI	✓	✓
Kontrolní prvky zabezpečení		
Kontrola aplikací	✓	✓
Kontrola zařízení	✓	–
Kontrola webu	✓	–
Adaptivní kontrola anomálií	✓	–
Šifrování dat		
Kaspersky Disk Encryption	✓	–
BitLocker Drive Encryption	✓	✓
Šifrování na úrovni souborů	✓	–
Šifrování vyměnitelných jednotek	✓	–
Endpoint Agent	✓	✓
Managed Detection and Response	✓	✓

Porovnání funkcí aplikace v závislosti na nástrojích správy

Soubor funkcí dostupných v aplikaci Kaspersky Endpoint Security závisí na nástrojích správy (viz tabulka níže).

Aplikaci můžete spravovat pomocí následujících konzolí aplikace Kaspersky Security Center 12:

- Konzola pro správu. Modul snap-in konzoly Microsoft Management Console (MMC) nainstalovaný na pracovní stanici správce.
- Webová konzola. Součást aplikace Kaspersky Security Center, která je nainstalována na serveru pro správu. Ve webové konzole můžete pracovat prostřednictvím prohlížeče na kterémkoli počítači, který má přístup k serveru pro správu.

Aplikaci můžete také spravovat pomocí cloudové konzole aplikace Kaspersky Security Center. *Cloudová konzola Kaspersky Security Center* je cloudová verze aplikace Kaspersky Security Center. To znamená, že server pro správu a další součásti aplikace Kaspersky Security Center jsou nainstalovány v cloudové infrastruktuře společnosti Kaspersky. Podrobné informace o správě aplikace prostřednictvím cloudové konzole aplikace Kaspersky Security Center *najdete v průvodci nápovědou ke cloudové konzole aplikace Kaspersky Security Center*.

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Kaspersky Security Center 12		Kaspersky Security Center
	Konzola pro správu	Webová konzola	Cloudová konzola
Rozšířená ochrana před hrozbami			
Služba hodnocení reputace KSN	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detekce chování	✓	✓	✓
Prevence zneužití	✓	✓	✓
Prevence narušení hostitele	✓	✓	✓
Modul pro nápravu	✓	✓	✓
Základní ochrana před hrozbami			
Ochrana před souborovými hrozbami	✓	✓	✓
Ochrana před webovými hrozbami	✓	✓	✓
Ochrana před hrozbami v poště	✓	✓	✓
Brána firewall	✓	✓	✓
Ochrana před síťovými hrozbami	✓	✓	✓
Ochrana před útoky BadUSB	✓	✓	✓
Managed Detection and Response	✓	✓	✓
Ochrana AMSI	✓	✓	✓
Kontrolní prvky zabezpečení			
Kontrola aplikací	✓	✓	✓

Kontrola zařízení	✓	✓	✓
Kontrola webu	✓	✓	✓
Adaptivní kontrola anomálií	✓	✓	✓
Šifrování dat			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption	✓	✓	✓
Šifrování na úrovni souborů	✓	✓	–
Šifrování vyměnitelných jednotek	✓	✓	–
Endpoint Agent	✓	✓	✓
Úlohy			
Přidat klíč	✓	✓	✓
Změna součásti aplikace	✓	✓	✓
Inventarizace	✓	✓	✓
Aktualizace	✓	✓	✓
Vrácení změn provedených aktualizací	✓	✓	✓
Antivirová kontrola	✓	✓	✓
Kontrola integrity	✓	✓	–
Vymazat data	✓	✓	✓
Správa účtů ověřovacího agenta	✓	✓	–

Kompatibilita s jinými aplikacemi

Aplikace Kaspersky Endpoint Security před instalací zkontroluje přítomnost aplikací společnosti Kaspersky v počítači. Aplikace také kontroluje nekompatibilní software v počítači. Seznam nekompatibilního softwaru je k dispozici v souboru incompatible.txt, který je zahrnut do distribuční sady.

STAŽENÍ NEKOMPATIBILNÍHO SOUBORU .TXT

Aplikace Kaspersky Endpoint Security není kompatibilní s následujícími aplikacemi společnosti Kaspersky:

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

- Kaspersky Anti Targeted Attack Platform (včetně součásti Endpoint Sensor).
- Kaspersky Sandbox (včetně součásti Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (včetně součásti Endpoint Sensor).

  Pokud byla součást Endpoint Agent nainstalována v počítači pomocí nástrojů pro nasazení jiných aplikací společnosti Kaspersky, bude tato součást během instalace aplikace Kaspersky Endpoint Security automaticky odebrána. Aplikace Kaspersky Endpoint Security může také zahrnovat součást Endpoint Sensor nebo Kaspersky Endpoint Agent, pokud jste v seznamu součástí aplikace vybrali Endpoint Agent.

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

Pokud jsou v počítači nainstalovány aplikace společnosti Kaspersky z tohoto seznamu, aplikace Kaspersky Endpoint Security tyto aplikace odebere. Počkejte, až bude tento proces dokončen, a poté pokračujte v instalaci aplikace Kaspersky Endpoint Security.

Instalace a odebrání aplikace

Aplikaci Kaspersky Endpoint Security lze do počítače instalovat několika způsoby:

- místně pomocí průvodce instalací,
- místně z příkazového řádku,
- vzdáleně prostřednictvím aplikace Kaspersky Security Center 12,
- vzdáleně prostřednictvím editoru správy zásad skupiny v systému Microsoft Windows (další podrobnosti viz *web technické podpory společnosti Microsoft*),
- vzdáleně pomocí aplikace System Center Configuration Manager.

Nastavení instalace aplikace můžete konfigurovat několika způsoby. Pokud současně používáte více způsobů pro konfiguraci nastavení, aplikace Kaspersky Endpoint Security použije nastavení s nejvyšší prioritou. Aplikace Kaspersky Endpoint Security používá následující pořadí priorit:

1. Nastavení přijatá ze souboru setup.ini.
2. Nastavení přijatá ze souboru installer.ini.
3. Nastavení přijatá z příkazového řádku.

Před zahájením instalace aplikace Kaspersky Endpoint Security doporučujeme ukončit všechny spuštěné aplikace (to se týká i vzdálené instalace).

Nasazení prostřednictvím aplikace Kaspersky Security Center 12

Aplikaci Kaspersky Endpoint Security lze nasadit do počítačů v podnikové síti několika způsoby. Můžete vybrat nejvhodnější scénář nasazení pro vaši organizaci nebo zkombinovat současně několik scénářů nasazení. Kaspersky Security Center 12 podporuje následující hlavní způsoby nasazení:

- Instalace aplikace pomocí průvodce Protection Deployment Wizard.

  Standardní způsob instalace je praktický, pokud jste spokojeni s výchozími nastaveními aplikace Kaspersky Endpoint Security a vaše organizace má jednoduchou infrastrukturu, která nevyžaduje speciální konfigurace.

- Instalace aplikace pomocí úlohy vzdálené instalace.

  Univerzální způsob instalace, který umožňuje konfiguraci nastavení aplikace Kaspersky Endpoint Security a flexibilní správu úloh vzdálené instalace. Instalace aplikace Kaspersky Endpoint Security se skládá z následujících kroků:

  1. vytvoření instalačního balíčku,
  2. vytvoření úlohy vzdálené instalace.

Aplikace Kaspersky Security Center 12 také podporuje jiné způsoby instalace aplikace Kaspersky Endpoint Security, jako je nasazení v rámci bitové kopie operačního systému. Podrobnosti o jiných způsobech nasazení *najdete v nápovědě k aplikaci Kaspersky Security Center 12*.

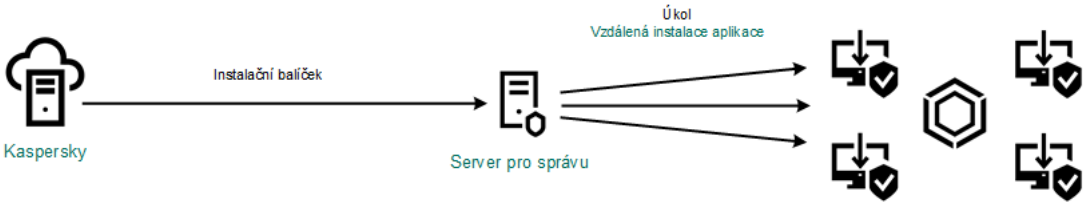
Standardní instalace aplikace

Aplikace Kaspersky Security Center poskytuje průvodce zavedením ochrany pro účely instalace aplikace do podnikových počítačů. Průvodce Protection Deployment Wizard obsahuje následující hlavní akce:

1. Výběr instalačního balíčku aplikace Kaspersky Endpoint Security.

   Instalační balíček je sada souborů vytvořených pro vzdálenou instalaci aplikace společnosti Kaspersky pomocí aplikace Kaspersky Security Center. Instalační balíček obsahuje řadu nastavení potřebných k instalaci aplikace a k jejímu spuštění okamžitě po instalaci. Instalační balíček je vytvořen pomocí souborů s příponami .kpd a .kud, které jsou obsaženy v distribučním balíčku aplikace. Instalační balíček aplikace Kaspersky Endpoint Security je společný pro všechny podporované verze systému Windows a typy architektur procesorů.

2. Vytvoření úlohy *Vzdálená instalace aplikace* serveru pro správu aplikace Kaspersky Security Center.



Nasazení aplikace Kaspersky Endpoint Security

[Jak spustit průvodce zavedením ochrany v konzole pro správu (MMC)]

1. V konzole pro správu přejděte do složky **Server pro správu** → **Další** → **Vzdálená instalace**.
2. Klikněte na odkaz **Nasadit instalační balíček na spravovaných zařízeních (pracovních stanicích)**.

Spustí se průvodce Security Deployment Wizard. Postupujte podle pokynů průvodce.

V klientském počítači je nutné otevřít porty TCP 139 a 445 a porty UDP 137 a 138.

Krok 1. Výběr instalačního balíčku

Ze seznamu vyberte instalační balíček aplikace Kaspersky Endpoint Security. Pokud seznam neobsahuje instalační balíček aplikace Kaspersky Endpoint Security, můžete balíček vytvořit v průvodci.

Nastavení instalačního balíčku můžete nakonfigurovat v aplikaci Kaspersky Security Center. Například můžete vybrat součásti aplikace, které se nainstalují do počítače.

Společně s aplikací Kaspersky Endpoint Security se také nainstaluje Network Agent. Součást *Network Agent* usnadňuje interakci mezi serverem pro správu a klientským počítačem. Pokud je již součást Network Agent v počítači nainstalována, znovu se nenainstaluje.

Step 2. Výběr zařízení pro instalaci

Vyberte počítače, do kterých se nainstaluje aplikace Kaspersky Endpoint Security. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Součást Network Agent není nainstalována do nepřiřazených zařízení. V tomto případě je úloha přiřazena ke konkrétním zařízením. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 3. Definování nastavení úlohy vzdálené instalace

Nakonfigurujte následující další nastavení aplikace:

- **Vynutit stažení instalačního balíčku**. Vyberte způsob instalace aplikace:
  - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
  - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Instalační balíček je do klientských počítačů doručeny prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.

- **Pomocí prostředků operačního systému prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému přes server pro správu. Tuto možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.

- **Chování zařízení spravovaných jinými servery**. Vyberte způsob instalace aplikace Kaspersky Endpoint Security. Pokud je v síti nainstalován více než jeden server pro správu, tyto servery pro správu mohou vidět stejné klientské počítače. To může například způsobit, že aplikace bude několikrát vzdáleně nainstalována do stejného klientského počítače pomocí různých serverů pro správu, případně jiné konflikty.

- **Do not install application if it is already installed**. Zrušte zaškrtnutí tohoto políčka, pokud chcete například nainstalovat starší verzi aplikace.

- **Assign Network Agent installation in the Active Directory group policies**. Ruční instalace součásti Network Agent pomocí prostředků služby Active Directory. Chcete-li nainstalovat součást Network Agent, je nutné spustit úlohu vzdálené instalace s oprávněními správce domény.

Krok 4. Výběr licenčního klíče

Přidejte klíč do instalačního balíčku, abyste aktivovali aplikaci. Tento krok je nepovinný. Pokud server pro správu obsahuje licenční klíč s funkcí automatické distribuce, klíč bude automaticky přidán později. Také můžete aplikaci aktivovat později pomocí úlohy *Přidat klíč*.

Krok 5. Výběr nastavení restartování operačního systému

Vyberte akci, která má být provedena, pokud je vyžadováno restartování počítače. Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Restartování je vyžadováno pouze v případě, že je nutné před instalací odebrat nekompatibilní aplikace. Restartování může být také vyžadováno při aktualizaci verze aplikace.

Krok 6. Odebrání nekompatibilních aplikací před instalací aplikace

Důkladně si přečtěte seznam nekompatibilních aplikací a povolte odebrání těchto aplikací. Pokud jsou v počítači nainstalovány nekompatibilní aplikace, instalace aplikace Kaspersky Endpoint Security skončí chybou.

Krok 7. Výběr účtu pro přístup k zařízením

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Pokud instalujete aplikaci Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 8. Zahájení instalace

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Nespouštět úlohu po dokončení průvodce vzdálenou instalací**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak spustit průvodce zavedením ochrany ve webové konzole a cloudové konzole

V hlavním okně webové konzoly vyberte možnosti **Device discovery and deployment** → **Deployment and assignment** → **Security Deployment Wizard**.

Spustí se průvodce Security Deployment Wizard. Postupujte podle pokynů průvodce.

V klientském počítači je nutné otevřít porty TCP 139 a 445 a porty UDP 137 a 138.

Krok 1. Výběr instalačního balíčku

Ze seznamu vyberte instalační balíček aplikace Kaspersky Endpoint Security. Pokud seznam neobsahuje instalační balíček aplikace Kaspersky Endpoint Security, můžete balíček vytvořit v průvodci. Chcete-li vytvořit instalační balíček, nemusíte hledat distribuční balíček a ukládat jej do paměti počítače. V aplikaci Kaspersky Security Center můžete zobrazit seznam distribučních balíčků nacházejících se na serverech společnosti Kaspersky a instalační balíček se automaticky vytvoří. Po vydání nových verzí aplikací společnost Kaspersky seznam aktualizuje.

Nastavení instalačního balíčku můžete nakonfigurovat v aplikaci Kaspersky Security Center. Například můžete vybrat součásti aplikace, které se nainstalují do počítače.

Krok 2. Výběr licenčního klíče

Přidejte klíč do instalačního balíčku, abyste aktivovali aplikaci. Tento krok je nepovinný. Pokud server pro správu obsahuje licenční klíč s funkcí automatické distribuce, klíč bude automaticky přidán později. Také můžete aplikaci aktivovat později pomocí úlohy *Přidat klíč*.

Krok 3. Výběr součásti Network Agent

Vyberte verzi součásti Network Agent, která se nainstaluje společně s aplikací Kaspersky Endpoint Security. Součást *Network Agent* usnadňuje interakci mezi serverem pro správu a klientským počítačem. Pokud je již součást Network Agent v počítači nainstalována, znovu se nenainstaluje.

Step 4. Výběr zařízení pro instalaci

Vyberte počítače, do kterých se nainstaluje aplikace Kaspersky Endpoint Security. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Součást Network Agent není nainstalována do nepřiřazených zařízení. V tomto případě je úloha přiřazena ke konkrétním zařízením. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Step 5. Konfigurace rozšířených nastavení

Nakonfigurujte následující další nastavení aplikace:

- **Vynutit stažení instalačního balíčku**. Výběr způsobu instalace aplikace:
  - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
  - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Instalační balíček je do klientských počítačů doručeny prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.
  - **Pomocí prostředků operačního systému prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému přes server pro správu. Tuto možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.
- **Do not install application if it is already installed**. Zrušte zaškrtnutí tohoto políčka, pokud chcete například nainstalovat starší verzi aplikace.
- **Assign package installation in Active Directory group policies**. Aplikace Kaspersky Endpoint Security je nainstalována pomocí součásti Network Agent nebo ručně pomocí služby Active Directory. Chcete-li nainstalovat součást Network Agent, je nutné spustit úlohu vzdálené instalace s oprávněními správce domény.

Krok 6. Výběr nastavení restartování operačního systému

Vyberte akci, která má být provedena, pokud je vyžadováno restartování počítače. Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Restartování je vyžadováno pouze v případě, že je nutné před instalací odebrat nekompatibilní aplikace. Restartování může být také vyžadováno při aktualizaci verze aplikace.

Krok 7. Odebrání nekompatibilních aplikací před instalací aplikace

Důkladně si přečtěte seznam nekompatibilních aplikací a povolte odebrání těchto aplikací. Pokud jsou v počítači nainstalovány nekompatibilní aplikace, instalace aplikace Kaspersky Endpoint Security skončí chybou.

Step 8. Přiřazení ke skupině pro správu

Vyberte skupinu pro správu, do které budou po instalaci součásti Network Agent počítače přesunuty. Počítače je třeba přesunout do skupiny pro správu, aby bylo možné aplikovat zásady a skupinové úlohy. Pokud je počítač již v nějaké skupině pro správu, nebude přesunut. Pokud nevyberte skupinu pro správu, počítače budou přidány do skupiny **Unassigned devices**.

Krok 9. Výběr účtu pro přístup k zařízením

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Pokud instalujete aplikaci Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 10. Spuštění instalace

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Vytvoření instalačního balíčku

Instalační balíček je sada souborů vytvořených pro vzdálenou instalaci aplikace společnosti Kaspersky pomocí aplikace Kaspersky Security Center. Instalační balíček obsahuje řadu nastavení potřebných k instalaci aplikace a k jejímu spuštění okamžitě po instalaci. Instalační balíček je vytvořen pomocí souborů s příponami .kpd a .kud, které jsou obsaženy v distribučním balíčku aplikace. Instalační balíček aplikace Kaspersky Endpoint Security je společný pro všechny podporované verze systému Windows a typy architektur procesorů.

Jak vytvořit instalační balíček v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Další** → **Vzdálená instalace** → **Instalační balíčky**.

   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.

2. Klikněte na tlačítko **Vytvořit instalační balíček**.

Spustí se průvodce novým balíčkem. Postupujte podle pokynů průvodce.

Krok 1. Výběr typu instalačního balíčku

Vyberte možnost **Vytvořit instalační balíček pro aplikaci Kaspersky**.

Krok 2. Definice názvu instalačního balíčku

Zadejte název instalačního balíčku, například `Kaspersky Endpoint Security pro systém Windows 11.6.0`.

Krok 3. Výběr distribučního balíčku pro instalaci

Klikněte na tlačítko **Procházet** a vyberte soubor `kes_win.kud`, který je součástí distribuční sady.

V případě potřeby aktualizujte antivirové databáze v instalačním balíčku pomocí zaškrtávacího políčka **Kopírovat aktualizace z úložiště do instalačního balíčku**.

Krok 4. Licenční smlouva s koncovým uživatelem a zásady ochrany osobních údajů

Přečtěte si a přijměte podmínky licenční smlouvy s koncovým uživatelem a zásad ochrany osobních údajů.

Vytvoří se instalační balíček a bude přidán do aplikace Kaspersky Security Center. Pomocí instalačního balíčku můžete nainstalovat aplikaci Kaspersky Endpoint Security do počítačů v podnikové síti nebo aktualizovat verzi aplikace. V nastavení instalačního balíčku můžete také vybrat součásti aplikace a nakonfigurovat nastavení instalace aplikace (viz tabulka níže). Instalační balíček obsahuje antivirové databáze z úložiště serveru pro správu. Můžete aktualizovat databáze v instalačním balíčku a snížit tak spotřebu provozu při aktualizaci databází po instalaci aplikace Kaspersky Endpoint Security.

Jak vytvořit instalační balíček ve webové konzole a cloudové konzole

1. V hlavním okně webové konzole vyberte možnosti **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.

   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.

2. Klikněte na tlačítko **Přidat**.

Spustí se průvodce novým balíčkem. Postupujte podle pokynů průvodce.

Krok 1. Výběr typu instalačního balíčku

Vyberte možnost **Vytvořit instalační balíček pro aplikaci Kaspersky**.

Průvodce vytvoří instalační balíček z distribučního balíčku umístěného na serverech společnosti Kaspersky. Jakmile jsou vydány nové verze aplikací, seznam je automaticky aktualizován. Pro instalaci aplikace Kaspersky Endpoint Security doporučujeme vybrat tuto možnost.

Můžete také vytvořit instalační balíček ze souboru.

Krok 2. Instalační balíčky

Vyberte instalační balíček aplikace Kaspersky Endpoint Security pro systém Windows. Spustí se proces vytvoření instalačního balíčku. Během vytváření instalačního balíčku musíte přijmout podmínky licenční smlouvy s koncovým uživatelem a oznámení o ochraně osobních údajů.

Vytvoří se instalační balíček a bude přidán do aplikace Kaspersky Security Center. Pomocí instalačního balíčku můžete nainstalovat aplikaci Kaspersky Endpoint Security do počítačů v podnikové síti nebo aktualizovat verzi aplikace. V nastavení instalačního balíčku můžete také vybrat součásti aplikace a nakonfigurovat nastavení instalace aplikace (viz tabulka níže). Instalační balíček obsahuje antivirové databáze z úložiště serveru pro správu. Můžete aktualizovat databáze v instalačním balíčku a snížit tak spotřebu provozu při aktualizaci databází po instalaci aplikace Kaspersky Endpoint Security.

Nastavení instalačního balíčku

Část	Popis
Součásti ochrany	V této části můžete vybrat součásti aplikace, které budou k dispozici. Později můžete změnit sadu součástí aplikace pomocí úlohy *Změnit součásti aplikace*. Součást Ochrana před útoky BadUSB, součást Endpoint Agent a součásti šifrování dat nejsou ve výchozím nastavení nainstalovány. Tyto součásti lze přidat v nastaveních instalačního balíčku.
Nastavení instalace	**Přidat umístění aplikace do proměnné prostředí %PATH%**. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku. **Nechránit proces instalace**. Ochrana instalace zahrnuje ochranu proti nahrazení distribučního balíčku škodlivými aplikacemi, blokování přístupu k instalační složce aplikace Kaspersky Endpoint Security a blokování přístupu k části systémového registru, která obsahuje klíče aplikace. Pokud však aplikaci nelze nainstalovat (například při vzdálené instalaci za použití funkce Vzdálená plocha systému Windows), doporučujeme ochranu instalace vypnout. **Zajistit kompatibilitu se službami Citrix PVS**. Můžete povolit podporu služeb Citrix Provisioning Services za účelem instalace aplikace Kaspersky Endpoint Security do virtuálního počítače. **Cesta k instalační složce aplikace**. Můžete změnit cestu instalace aplikace Kaspersky Endpoint Security v klientském počítači. Ve výchozím nastavení je aplikace nainstalována do složky `%ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows`.

	Konfigurační soubor. Můžete nahrát soubor, který definuje nastavení aplikace Kaspersky Endpoint Security. Můžete vytvořit konfigurační soubor v místním rozhraní aplikace.

Aktualizace databází v instalačním balíčku

Instalační balíček obsahuje antivirové databáze z úložiště serveru pro správu, které jsou aktuální při vytváření instalačního balíčku. Po vytvoření instalačního balíčku můžete antivirové databáze v instalačním balíčku aktualizovat. To vám umožní snížit spotřebu provozu při aktualizaci antivirových databází po instalaci aplikace Kaspersky Endpoint Security.

Chcete-li aktualizovat antivirové databáze v úložišti serveru pro správu, použijte úlohu *Stáhnout aktualizace do úložiště serveru pro správu* na serveru pro správu. Další informace o aktualizaci antivirových databází v úložišti serveru pro správu najdete v *nápovědě k aplikaci Kaspersky Security Center*.

Databáze v instalačním balíčku můžete aktualizovat pouze v konzole pro správu a webové konzole aplikace Kaspersky Security Center 12. Databáze v instalačním balíčku nelze aktualizovat v cloudové konzole aplikace Kaspersky Security Center.

Jak aktualizovat antivirové databáze v instalačním balíčku pomocí konzoly pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Další** → **Vzdálená instalace** → **Instalační balíčky**.

   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.

2. Otevřete vlastnosti instalačního balíčku.

3. V části **Obecné** klikněte na tlačítko **Aktualizovat databáze**.

Tím aktualizujete antivirové databáze v instalačním balíčku z úložiště serveru pro správu. Soubor `bases.cab`, který je součástí distribuční sady, bude nahrazen složkou `bases`. Soubory aktualizačního balíčku budou uvnitř složky.

Jak aktualizovat antivirové databáze v instalačním balíčku prostřednictvím webové konzoly

1. V hlavním okně webové konzole vyberte možnosti **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.

   Otevře se seznam instalačních balíčků stažených do webové konzole.

2. Klikněte na název instalačního balíčku aplikace Kaspersky Endpoint Security, ve kterém chcete aktualizovat antivirové databáze.

   Otevře se okno vlastností serveru pro správu.

3. Na kartě **Obecné informace** klikněte na odkaz **Aktualizovat databáze**.

Tím aktualizujete antivirové databáze v instalačním balíčku z úložiště serveru pro správu. Soubor `bases.cab`, který je součástí distribuční sady, bude nahrazen složkou `bases`. Soubory aktualizačního balíčku budou uvnitř složky.

Vytvoření úlohy vzdálené instalace

Úloha *Vzdálená instalace aplikace* je určena pro vzdálenou instalaci aplikace Kaspersky Endpoint Security. Úloha *Vzdálená instalace aplikace* vám umožňuje nasadit instalační balíček aplikace do všech počítačů v organizaci. Před nasazením instalačního balíčku můžete aktualizovat antivirové databáze uvnitř balíčku a vybrat ve vlastnostech instalačního balíčku dostupné součásti aplikace.

Jak vytvořit úlohu vzdálené instalace v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte položky **Server pro správu Kaspersky Security Center** → **Vzdálená instalace aplikace**.

Krok 2. Výběr instalačního balíčku

Ze seznamu vyberte instalační balíček aplikace Kaspersky Endpoint Security. Pokud seznam neobsahuje instalační balíček aplikace Kaspersky Endpoint Security, můžete balíček vytvořit v průvodci.

Nastavení instalačního balíčku můžete nakonfigurovat v aplikaci Kaspersky Security Center. Například můžete vybrat součásti aplikace, které se nainstalují do počítače.

Společně s aplikací Kaspersky Endpoint Security se také nainstaluje Network Agent. Součást *Network Agent* usnadňuje interakci mezi serverem pro správu a klientským počítačem. Pokud je již součást Network Agent v počítači nainstalována, znovu se nenainstaluje.

Krok 3. Rozšířené

Vyberte instalační balíček součásti Network Agent. Vybraná verze součásti Network Agent se nainstaluje společně s aplikací Kaspersky Endpoint Security.

Krok 4. Nastavení

Nakonfigurujte následující další nastavení aplikace:

- **Vynutit stažení instalačního balíčku**. Vyberte způsob instalace aplikace:
  - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
  - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Instalační balíček je do klientských počítačů doručeny prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.
  - **Pomocí prostředků operačního systému prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému přes server pro správu. Tuto možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.
- **Chování zařízení spravovaných jinými servery**. Vyberte způsob instalace aplikace Kaspersky Endpoint Security. Pokud je v síti nainstalován více než jeden server pro správu, tyto servery pro správu mohou vidět

stejné klientské počítače. To může například způsobit, že aplikace bude několikrát vzdáleně nainstalována do stejného klientského počítače pomocí různých serverů pro správu, případně jiné konflikty.

- **Do not install application if it is already installed**. Zrušte zaškrtnutí tohoto políčka, pokud chcete například nainstalovat starší verzi aplikace.

Krok 5. Výběr nastavení restartování operačního systému

Vyberte akci, která má být provedena, pokud je vyžadováno restartování počítače. Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Restartování je vyžadováno pouze v případě, že je nutné před instalací odebrat nekompatibilní aplikace. Restartování může být také vyžadováno při aktualizaci verze aplikace.

Krok 6. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, do kterých se nainstaluje aplikace Kaspersky Endpoint Security. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.

- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Součást Network Agent není nainstalována do nepřiřazených zařízení. V tomto případě je úloha přiřazena ke konkrétním zařízením. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.

- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 7. Výběr účtu pro spuštění úlohy

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Pokud instalujete aplikaci Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 8. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně, nebo když je počítač nečinný.

Krok 9. Definování názvu úlohy

Zadejte název úlohy, například `Instalace Kaspersky Endpoint Security pro systém Windows 11.6.0`.

Krok 10. Vytvoření úloh po dokončení

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. Aplikace bude nainstalována v bezobslužném režimu. Po instalaci se bude do oznamovací oblasti počítače uživatele přidána ikona . Pokud ikona vypadá takto , ujistěte se, že jste aktivovali aplikaci.

Jak vytvořit úlohu vzdálené instalace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Aplikace** vyberte možnost **Kaspersky Security Center**.
2. V rozevíracím seznamu **Typ úlohy** vyberte možnost **vzdálené instalace aplikace**.
3. V poli **Task name** zadejte krátký popis, například `Instalace aplikace Kaspersky Endpoint Security pro správce`.
4. V části **Devices to which the task will be assigned** vyberte rozsah úlohy.

Step 2. Výběr počítačů pro instalaci

V tomto kroku vyberte počítače, na něž bude nainstalována aplikace Kaspersky Endpoint Security podle vybrané možnosti rozsahu úlohy.

Krok 3. Konfigurace instalačního balíčku

V tomto kroku nakonfigurujte nastavení instalačního balíčku**:**

1. Vyberte instalační balíček aplikace Kaspersky Endpoint Security pro systém Windows (11.6.0).
2. Vyberte instalační balíček součásti Network Agent.

   Vybraná verze součásti Network Agent se nainstaluje společně s aplikací Kaspersky Endpoint Security. Součást *Network Agent* usnadňuje interakci mezi serverem pro správu a klientským počítačem. Pokud je již součást Network Agent v počítači nainstalována, znovu se nenainstaluje.

3. V části **Force download of the installation package** vyberte způsob instalace aplikace:

   - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
   - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Instalační balíček je do klientských počítačů doručeny prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.
   - **Pomocí prostředků operačního systému prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému přes server pro správu. Tuto

možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.

4. V poli **Maximum number of simultaneous downloads** nastavte limit počtu požadavků na stažení instalačního balíčku, které jsou odeslány na server pro správu. Limit počtu požadavků pomůže zabránit přetížení sítě.

5. V poli **Number of installation attempts** nastavte limit počtu pokusů o instalaci aplikace. Pokud instalace aplikace Kaspersky Endpoint Security skončí chybou, úloha automaticky spustí instalaci znovu.

6. V případě potřeby zrušte zaškrtnutí políčka **Do not install application if it is already installed**. Umožňuje například nainstalovat některou z předchozích verzí aplikace.

7. V případě potřeby zrušte zaškrtnutí políčka **Check the operating system version before installation**. To umožňuje zabránit stažení distribučního balíčku aplikace, pokud operační systém počítače nesplňuje požadavky na software. Pokud si jste jisti, že operační systém počítače splňuje požadavky na software, můžete toto ověřování přeskočit.

8. V případě potřeby zaškrtněte políčko **Assign package installation in Active Directory group policies**. Aplikace Kaspersky Endpoint Security je nainstalována pomocí součásti Network Agent nebo ručně pomocí služby Active Directory. Chcete-li nainstalovat součást Network Agent, je nutné spustit úlohu vzdálené instalace s oprávněními správce domény.

9. V případě potřeby zaškrtněte políčko **Offer users to quit running applications**. Instalace aplikace Kaspersky Endpoint Security zabírá prostředky počítače. Z důvodu pohodlí pro uživatele vás Průvodce instalací aplikace vyzve, abyste před spuštěním instalace zavřeli spuštěné aplikace. To pomůže zabránit narušení fungování dalších aplikací a zabrání to možným selháním počítače.

10. V části **Chování zařízení spravovaných tímto serverem** vyberte způsob instalace aplikace Kaspersky Endpoint Security. Pokud je v síti nainstalován více než jeden server pro správu, tyto servery pro správu mohou vidět stejné klientské počítače. To může například způsobit, že aplikace bude několikrát vzdáleně nainstalována do stejného klientského počítače pomocí různých serverů pro správu, případně jiné konflikty.

Krok 4. Výběr účtu pro spuštění úlohy

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Pokud instalujete aplikaci Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 5. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Dokončit** dokončete průvodce. V seznamu úloh se zobrazí nová úloha. Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**. Aplikace bude nainstalována v bezobslužném režimu. Po instalaci se bude do oznamovací oblasti počítače uživatele přidána ikona . Pokud ikona vypadá takto , ujistěte se, že jste aktivovali aplikaci.

Místní instalace aplikace pomocí průvodce

Rozhraní průvodce instalací aplikace je tvořeno sledem oken, která odpovídají postupu instalace aplikace.

Postup instalace aplikace nebo upgradu aplikace ze starší verze pomocí průvodce instalací:

1. Zkopírujte složku distribuční sady do počítače uživatele.
2. Spusťte soubor setup_kes.exe.

Spustí se Průvodce instalací.

Příprava na instalaci

Před instalací aplikace Kaspersky Endpoint Security do počítače nebo jejím upgradem z předchozí verze jsou zkontrolovány následující podmínky:

- Přítomnost nainstalovaného nekompatibilního softwaru (seznam nekompatibilního softwaru je k dispozici v souboru incompatible.txt, který je součástí distribuční sady).
- Zda jsou či nejsou splněny požadavky na hardware a software.
- Zda uživatel má či nemá práva k instalaci softwarového produktu.

Pokud jakýkoli z předchozích požadavků není splněn, na obrazovce se objeví příslušné upozornění.

Jestliže počítač uvedené požadavky splňuje, průvodce instalací se pokusí najít aplikace společnosti Kaspersky, které by mohly způsobit konflikty při současném použití s instalovanou aplikací. Při nalezení takových aplikací budete vyzváni k jejich ručnímu odebrání.

Pokud jsou mezi zjištěnými aplikacemi obsaženy předchozí verze aplikace Kaspersky Endpoint Security, všechna data, která lze přenést (například aktivační data a nastavení aplikace), jsou zachována a použita během instalace aplikace Kaspersky Endpoint Security 11.6.0 pro systém Windows a předchozí verze aplikace je automaticky odebrána. To se týká následujících verzí aplikace:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 pro systém Windows (sestavení 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows (sestavení 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 pro systém Windows (sestavení 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 pro systém Windows (sestavení 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 pro systém Windows (sestavení 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 pro systém Windows (sestavení 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 pro systém Windows (sestavení 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 pro systém Windows (sestavení 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 pro systém Windows SF1 (sestavení 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 pro systém Windows (sestavení 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 pro systém Windows (sestavení 11.1.1.126).

- Kaspersky Endpoint Security 11.2.0 pro systém Windows (sestavení 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 pro systém Windows CF1 (sestavení 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 pro systém Windows (sestavení 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 pro systém Windows (sestavení 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 pro systém Windows (sestavení 11.5.0.590).

Součásti aplikace Kaspersky Endpoint Security

Během instalace můžete vybrat součásti aplikace Kaspersky Endpoint Security, které chcete nainstalovat. Součást Ochrana před souborovými hrozbami je povinná součást, kterou je nutné nainstalovat. Její instalaci nelze zrušit.

Ve výchozím nastavení jsou pro instalaci vybrány všechny součásti aplikace kromě těchto:

- Ochrana před útoky BadUSB.
- Šifrování na úrovni souborů.
- Úplné šifrování disku.
- BitLocker Management.
- Endpoint Agent. *Endpoint Agent* nainstaluje aplikaci Kaspersky Endpoint Agent 3.10 pro interakci mezi aplikací a řešeními společnosti Kaspersky pro detekci pokročilých hrozeb (například Kaspersky Sandbox).

Dostupné součásti aplikace můžete změnit po instalaci aplikace. Chcete-li tak učinit, musíte znovu spustit Průvodce nastavením a zvolit změnu dostupných součástí.

Rozšířené nastavení

Chránit proces instalace aplikace. Ochrana instalace zahrnuje ochranu proti nahrazení distribučního balíčku škodlivými aplikacemi, blokování přístupu k instalační složce aplikace Kaspersky Endpoint Security a blokování přístupu k části systémového registru, která obsahuje klíče aplikace. Pokud však aplikaci nelze nainstalovat (například při vzdálené instalaci za použití funkce Vzdálená plocha systému Windows), doporučujeme ochranu instalace vypnout.

Zajistit kompatibilitu se službami Citrix PVS. Můžete povolit podporu služeb Citrix Provisioning Services za účelem instalace aplikace Kaspersky Endpoint Security do virtuálního počítače.

Přidat umístění aplikace do proměnné prostředí %PATH%. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku.

Instalace aplikace z příkazového řádku

Aplikaci Kaspersky Endpoint Security lze nainstalovat z příkazového řádku v jednom z těchto režimů:

- V interaktivním režimu za použití průvodce instalací aplikace.

- V bezobslužném režimu. Po spuštění instalace v bezobslužném režimu nemusíte během instalace provádět žádnou činnost. Chcete-li nainstalovat aplikaci v bezobslužném režimu, použijte klávesy `/s` a `/qn`.

  Před instalací aplikace v bezobslužném režimu otevřete a přečtěte si licenční smlouvu s koncovým uživatelem a zásady ochrany osobních údajů. Licenční smlouva s koncovým uživatelem a text zásad ochrany osobních údajů jsou součástí distribuční sady aplikace Kaspersky Endpoint Security. V instalaci aplikace můžete pokračovat, pouze pokud jste si přečetli úplné znění podmínek licenční smlouvy s koncovým uživatelem, rozumíte jim a přijali je, chápete a souhlasíte s tím, že vaše údaje budou zpracovávány a předávány (včetně třetích zemí) v souladu se zásadami ochrany osobních údajů, a přečetli si úplné znění zásad ochrany osobních údajů a rozumíte jim. Pokud podmínky licenční smlouvy s koncovým uživatelem a zásad ochrany osobních údajů nepřijmete, neinstalujte ani nepoužívejte aplikaci Kaspersky Endpoint Security.

Chcete-li nainstalovat aplikaci nebo upgradovat předchozí verzi aplikace:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, kde se nachází distribuční balíček aplikace Kaspersky Endpoint Security.
3. Spusťte následující příkaz:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
   [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<uživatelské jméno>
   /pKLPASSWD=<heslo> /pKLPASSWDAREA=<rozsah hesla>] [/pENABLETRACES=1|0 /pTRACESLEVEL=
   <úroveň trasování>] [/s]
   ```

   nebo

   ```
   msiexec /i <název distribuční sady> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
   [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<uživatelské jméno> KLPASSWD=<heslo>
   KLPASSWDAREA=<rozsah hesla>] [ENABLETRACES=1|0 TRACESLEVEL=<úroveň trasování>] [/qn]
   ```

`EULA=1`	Přijetí podmínek licenční smlouvy s koncovým uživatelem. Text podmínek licenční smlouvy zahrnutý do distribučního balíčku aplikace Kaspersky Endpoint Security. Přijetí podmínek licenční smlouvy s koncovým uživatelem je nutné pro instalaci aplikace nebo upgrade její verze.
`PRIVACYPOLICY=1`	Přijetí zásad ochrany osobních údajů. Text zásad ochrany osobních údajů je součástí distribučního balíčku aplikace Kaspersky Endpoint Security. Chcete-li nainstalovat aplikaci nebo upgradovat verzi aplikace, je nutné přijmout zásady ochrany osobních údajů.
`KSN`	Přijetí nebo odmítnutí účasti ve službě Kaspersky Security Network (KSN). Pokud pro tento parametr není nastavena žádná hodnota, aplikace Kaspersky Endpoint Security při prvním spuštění zobrazí výzvu k potvrzení přijetí nebo odmítnutí účasti ve službě KSN. Dostupné hodnoty: • `1` – souhlas s účastí ve službě KSN. • `0` – odmítnutí účasti ve službě KSN (výchozí hodnota).

	Distribuční balíček Kaspersky Endpoint Security je optimalizován pro použití se službou Kaspersky Security Network. Pokud jste nesouhlasili s účastí ve službě Kaspersky Security Network, ihned po dokončení instalace je třeba aktualizovat aplikaci Kaspersky Endpoint Security.
`ALLOWREBOOT=1`	Automatický restart počítače po instalaci nebo upgradu aplikace, pokud je třeba. Pokud pro tento parametr není nastavena žádná hodnota, je automatický restart počítače blokován. Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Restartování je vyžadováno pouze v případě, že je nutné před instalací odebrat nekompatibilní aplikace. Restartování může být také vyžadováno při aktualizaci verze aplikace.
`SKIPPRODUCTCHECK=1`	Zákaz kontroly nekompatibilního softwaru. Seznam nekompatibilního softwaru je k dispozici v souboru incompatible.txt, který je zahrnut do distribuční sady. Pokud není u tohoto parametru nastavena žádná hodnota a je zjištěn nekompatibilní software, instalace aplikace Kaspersky Endpoint Security bude ukončena.
`SKIPPRODUCTUNINSTALL=1`	Zakázání automatického odebrání zjištěného nekompatibilního softwaru. Pokud není u tohoto parametru nastavena žádná hodnota, aplikace Kaspersky Endpoint Security se pokusí nekompatibilní software odebrat. Automatické odstranění nekompatibilního softwaru nelze povolit, pokud instalujete Kaspersky Endpoint Security pomocí instalačního programu msiexec. Pro povolení automatického odstranění nekompatibilního softwaru použijte program setup_kes.exe.
`KLLOGIN`	Nastavte uživatelské jméno pro přístup k funkcím a nastavením aplikace Kaspersky Endpoint Security (součást Ochrana heslem). Uživatelské jméno se nastavuje společně s parametry `KLPASSWD` a `KLPASSWDAREA`. Ve výchozím nastavení se použije uživatelské jméno KLAdmin.
`KLPASSWD`	Zadejte heslo pro přístup k funkcím a nastavením aplikace Kaspersky Endpoint Security (heslo se zadává společně s parametry `KLLOGIN` a `KLPASSWDAREA`). Pokud jste zadali heslo, ale nezadali jste uživatelské jméno společně s parametrem `KLLOGIN`, jako výchozí se použije uživatelské jméno KLAdmin.
`KLPASSWDAREA`	Zadejte rozsah hesla pro přístup k aplikaci Kaspersky Endpoint Security. Když se uživatel pokusí provést akci, která je zahrnuta v tomto rozsahu, aplikace Kaspersky Endpoint Security zobrazí výzvu k zadání přihlašovacích údajů k účtu uživatele (parametry `KLLOGIN` a `KLPASSWD`). Pomocí znaku „`;`“ zadejte více hodnot. Dostupné hodnoty: • `SET` – úprava nastavení aplikace. • `EXIT` – ukončení aplikace. • `DISPROTECT` – zakázání součástí ochrany a zastavení úloh kontroly. • `DISPOLICY` – zakázání zásad aplikace Kaspersky Security Center. • `UNINST` – odebrání aplikace z počítače.

	• `DISCTRL` – zakázání součástí kontroly. • `REMOVELIC` – odebrání klíče. • `REPORTS` – zobrazení zpráv.
`ENABLETRACES`	Povolí nebo zakáže trasování aplikací. Po spuštění uloží aplikace Kaspersky Endpoint Security soubory trasování do složky %ProgramData%/Kaspersky Lab\KES\Traces. Dostupné hodnoty: • `1` – je povoleno trasování aplikací. • `0` – je zakázáno trasování aplikací (výchozí hodnota).
`TRACESLEVEL`	Úroveň podrobností trasování. Dostupné hodnoty: • `100` (kritické). Pouze zprávy o závažných chybách. • `200` (vysoké). Zprávy o všech chybách, včetně závažných chyb. • `300` (diagnostické). Zprávy o všech chybách a varováních. • `400` (důležité). Všechny chybové zprávy, varování a další informace. • `500` (normální). Zprávy o všech chybách a varováních a podrobné informace o provozu aplikace v normálním režimu (výchozí). • `600` (nízké). Všechny zprávy.
`AMPPL`	Povolí nebo zakáže ochranu procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL (Antimalware Protected Process Light). Podrobnější informace o fungování technologie AM-PPL najdete na webu společnosti Microsoft. Technologie AM-PPL je k dispozici pro operační systémy Windows 10 verze 1703 (RS2) nebo novější a pro operační systémy Windows Server 2019. Dostupné hodnoty: • `1` – je povolena ochrana procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL. • `0` – je zakázána ochrana procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL.
`RESTAPI`	Správa aplikace prostřednictvím rozhraní REST API. Chcete-li spravovat aplikaci pomocí rozhraní REST API, musíte zadat uživatelské jméno (parametr `RESTAPI_User`). Dostupné hodnoty: • `1` – správa přes REST API je povolena. • `0` – správa přes REST API je blokována (výchozí hodnota).

	Chcete-li spravovat aplikaci pomocí rozhraní REST API, musí být povolena správa pomocí administrativních systémů. To provedete nastavením parametru `AdminKitConnector=1`. Pokud spravujete aplikaci pomocí REST API, není možné spravovat aplikaci pomocí systémů pro správu společnosti Kaspersky.
`RESTAPI_User`	Uživatelské jméno účtu domény systému Windows použitého pro správu aplikace prostřednictvím rozhraní REST API. Správa aplikace prostřednictvím rozhraní REST API je k dispozici pouze pro tohoto uživatele. Zadejte uživatelské jméno ve formátu `<DOMAIN>\<UserName>` (například `RESTAPI_User=COMPANY\Administrator`). Pro práci s rozhraním REST API můžete vybrat pouze jednoho uživatele. Předpokladem pro správu aplikace prostřednictvím rozhraní REST API je přidání uživatelského jména.
`RESTAPI_Port`	Port používaný pro správu aplikace prostřednictvím rozhraní REST API. Ve výchozím nastavení je použit port 6782.
`ADMINKITCONNECTOR`	Správa aplikací pomocí systémů pro správu. Mezi systémy pro správu patří například Kaspersky Security Center. Kromě systémů pro správu společnosti Kaspersky můžete také používat řešení třetích stran. Aplikace Kaspersky Endpoint Security poskytuje k těmto účelům rozhraní API. Dostupné hodnoty: • `1` – správa aplikací je povolena pomocí systémů pro správu (výchozí hodnota). • `0` – správa aplikací je povolena pouze prostřednictvím lokálního rozhraní.

Příklad:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1

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

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

Po instalaci aplikace Kaspersky Endpoint Security se aktivuje zkušební licence, ledaže jste v souboru setup.ini zadali aktivační kód. Zkušební licence je obvykle krátkodobá. Když platnost zkušební licence skončí, všechny funkce aplikace Kaspersky Endpoint Security se zakážou. Chcete-li pokračovat v používání aplikace, musíte aktivovat aplikaci pomocí komerční licence prostřednictvím průvodce aktivací aplikace nebo zvláštním příkazem.

Při instalaci aplikace nebo upgradování její verze v bezobslužném režimu je podporováno použití následujících souborů:

- setup.ini – obecná nastavení instalace aplikace
- install.cfg – nastavení činnosti aplikace Kaspersky Endpoint Security
- setup.reg – klíče registru

Klíče registru ze souboru setup.reg jsou zapsány do registru pouze v případě, že v souboru setup.ini je pro parametr `SetupReg` nastavena hodnota `setup.reg`. Soubor setup.reg je vygenerován odborníky společnosti Kaspersky. Nedoporučuje se měnit obsah tohoto souboru.

Chcete-li použít nastavení ze souborů setup.ini, install.cfg a setup.reg, umístěte tyto soubory do složky, která obsahuje distribuční balíček aplikace Kaspersky Endpoint Security. Soubor setup.reg můžete také umístit do jiné složky. Pokud tak učiníte, musíte zadat cestu k souboru v následujícím instalačním příkazu aplikace: `SETUPREG=<cesta k souboru setup.reg>`.

Vzdálená instalace aplikace pomocí aplikace System Center Configuration Manager

Tyto pokyny platí pro verzi System Center Configuration Manager 2012 R2.

Postup vzdálené instalace aplikace pomocí aplikace System Center Configuration Manager:

1. Otevřete konzoli Configuration Manager.
2. V pravé části konzole vyberte v části **App management** položku **Packages**.
3. V horní části konzole klikněte na ovládacím panelu na tlačítko **Create package**.
   Spustí se průvodce *New Package and Application Wizard*.
4. V průvodci New Package and Application Wizard:
   a. V části **Package**:
      - V poli **Name** zadejte název instalačního balíčku.
      - V poli **Source folder** zadejte cestu ke složce obsahující distribuční sadu aplikace Kaspersky Endpoint Security.
   b. V části **Application type** vyberte možnost **Standard application**.
   c. V části **Standard application**:
      - V poli **Name** zadejte jedinečný název instalačního balíčku (například název aplikace včetně verze).
      - V poli **Command line** určete možnosti instalace aplikace Kaspersky Endpoint Security z příkazového řádku.
      - Klikněte na tlačítko **Browse** a určete cestu ke spustitelnému souboru aplikace.
      - Ujistěte se, že u seznamu **Execution mode** je vybrána položka **Run with administrator rights**.
   d. V části **Requirements**:
      - Zaškrtněte políčko **Start another application first**, pokud chcete, aby byla před instalací aplikace Kaspersky Endpoint Security spuštěna jiná aplikace.

Vyberte aplikaci v rozevíracím seznamu **Application** nebo určete cestu ke spustitelnému souboru aplikace po kliknutí na tlačítko **Browse**.

- Pokud si přejete, aby byla aplikace nainstalována pouze do určených operačních systémů, vyberte možnost **This application can be started only on the specified platforms** v části **Platform requirements**.

  V níže uvedeném seznamu zaškrtněte políčka vedle operačních systémů, do kterých bude aplikace Kaspersky Endpoint Security nainstalována.

Tento krok je nepovinný.

e. V části **Summary** zkontrolujte veškeré zadané hodnoty nastavení a klikněte na tlačítko **Next**.

Vytvořený instalační balíček se zobrazí v části **Packages** v seznamu dostupných instalačních balíčků.

5. V kontextové nabídce instalačního balíčku vyberte možnost **Deploy**.

   Spustí se průvodce *Deployment Wizard*.

6. V průvodci Deployment Wizard:

   a. V části **General**:

   - V poli **Software** zadejte jedinečný název instalačního balíčku nebo vyberte instalační balíček ze seznamu kliknutím na tlačítko **Browse**.
   - V poli **Collection** zadejte název skupiny počítačů, do kterých má být aplikace nainstalována, nebo skupinu vyberte kliknutím na tlačítko **Browse**.

   b. V části **Contains** přidejte distribuční body (podrobnější informace najdete v nápovědě aplikace System Center Configuration Manager).

   c. Pokud je to třeba, určete hodnoty dalších nastavení v průvodci Deployment Wizard. Tato nastavení jsou pro vzdálenou instalaci aplikace Kaspersky Endpoint Security nepovinná.

   d. V části **Summary** zkontrolujte veškeré zadané hodnoty nastavení a klikněte na tlačítko **Next**.

   Po dokončení průvodce Deployment Wizard bude vytvořena úloha pro vzdálenou instalaci aplikace Kaspersky Endpoint Security.

Popis nastavení instalace souboru setup.ini

Soubor setup.ini se používá při instalaci aplikace z příkazového řádku nebo při použití editoru zásad skupiny v systému Microsoft Windows. Chcete-li použít nastavení ze souboru setup.ini, umístěte tento soubor do složky, která obsahuje distribuční balíček aplikace Kaspersky Endpoint Security.

STAŽENÍ SOUBORU .INI

Soubor setup.ini se skládá z následujících částí:

- `[Setup]` – obecná nastavení instalace aplikace.
- `[Components]` – výběr součástí aplikace, které se mají instalovat. Pokud nejsou zadány žádné součásti, nainstalují se všechny součásti, které jsou dostupné pro daný operační systém. Ochrana před souborovými

hrozbami je povinná součást a je nainstalována do počítače bez ohledu na to, jaká nastavení jsou určena v této části. Součást Managed Detection and Response také v této části chybí. Chcete-li součást Managed Detection a Response nainstalovat, musíte ji aktivovat v konzole aplikace Kaspersky Security Center.

- `[Tasks]` – výběr úloh, které mají být přidány na seznam úloh aplikace Kaspersky Endpoint Security. Pokud není zadána žádná úloha, na seznam úloh aplikace Kaspersky Endpoint Security budou přidány všechny úlohy.

Místo hodnoty `1` lze použít hodnoty `yes`, `on`, `enable` a `enabled`.

Místo hodnoty `0` lze použít hodnoty `no`, `off`, `disable` a `disabled`.

Nastavení souboru setup.ini

Část	Parametr	Popis
`[Setup]`	`InstallDir`	Cesta k instalační složce aplikace.
	`ActivationCode`	Aktivační kód aplikace Kaspersky Endpoint Security.
	`EULA=1`	Přijetí podmínek licenční smlouvy s koncovým uživatelem. Text podmínek licenční smlouvy zahrnutý do distribučního balíčku aplikace Kaspersky Endpoint Security. Přijetí podmínek licenční smlouvy s koncovým uživatelem je nutné pro instalaci aplikace nebo upgrade její verze.
	`PrivacyPolicy=1`	Přijetí zásad ochrany osobních údajů. Text zásad ochrany osobních údajů je součástí distribučního balíčku aplikace Kaspersky Endpoint Security. Chcete-li nainstalovat aplikaci nebo upgradovat verzi aplikace, je nutné přijmout zásady ochrany osobních údajů.
	`KSN`	Přijetí nebo odmítnutí účasti ve službě Kaspersky Security Network (KSN). Pokud pro tento parametr není nastavena žádná hodnota, aplikace Kaspersky Endpoint Security při prvním spuštění zobrazí výzvu k potvrzení přijetí nebo odmítnutí účasti ve službě KSN. Dostupné hodnoty: • `1` – souhlas s účastí ve službě KSN. • `0` – odmítnutí účasti ve službě KSN (výchozí hodnota).

		Distribuční balíček Kaspersky Endpoint Security je optimalizován pro použití se službou Kaspersky Security Network. Pokud jste nesouhlasili s účastí ve službě Kaspersky Security Network, ihned po dokončení instalace je třeba aktualizovat aplikaci Kaspersky Endpoint Security.
	`Login`	Nastavte uživatelské jméno pro přístup k funkcím a nastavením aplikace Kaspersky Endpoint Security (součást Ochrana heslem). Uživatelské jméno se nastavuje společně s nastaveními `Password` a `PasswordArea`. Ve výchozím nastavení se použije uživatelské jméno KLAdmin.
	`Password`	Zadejte heslo pro přístup k funkcím a nastavením aplikace Kaspersky Endpoint Security (heslo se zadává společně s parametry `Login` a `PasswordArea`). Pokud jste zadali heslo, ale nezadali jste uživatelské jméno společně s parametrem `Login`, jako výchozí se použije uživatelské jméno KLAdmin.
	`PasswordArea`	Zadejte rozsah hesla pro přístup k aplikaci Kaspersky Endpoint Security. Když se uživatel pokusí provést akci, která je zahrnuta v tomto rozsahu, aplikace Kaspersky Endpoint Security zobrazí výzvu k zadání přihlašovacích údajů k účtu uživatele (parametry `Login` a `Password`). Pomocí znaku „`;`“ zadejte více hodnot. Dostupné hodnoty: • `SET` – úprava nastavení aplikace. • `EXIT` – ukončení aplikace. • `DISPROTECT` – zakázání součástí ochrany a zastavení úloh kontroly. • `DISPOLICY` – zakázání zásad aplikace Kaspersky Security Center. • `UNINST` – odebrání aplikace z počítače. • `DISCTRL` – zakázání součástí kontroly. • `REMOVELIC` – odebrání klíče. • `REPORTS` – zobrazení zpráv.
	`SelfProtection`	Povolení nebo zakázání mechanismu ochrany instalace aplikace. Dostupné hodnoty: • `1` – mechanismus ochrany instalace aplikace je povolený (výchozí hodnota). • `0` – mechanismus ochrany instalace aplikace je zakázaný.

		Ochrana instalace zahrnuje ochranu proti nahrazení distribučního balíčku škodlivými aplikacemi, blokování přístupu k instalační složce aplikace Kaspersky Endpoint Security a blokování přístupu k části systémového registru, která obsahuje klíče aplikace. Pokud však aplikaci nelze nainstalovat (například při vzdálené instalaci za použití funkce Vzdálená plocha systému Windows), doporučujeme ochranu instalace vypnout.
	`Reboot=1`	Automatický restart počítače po instalaci nebo upgradu aplikace, pokud je třeba. Pokud pro tento parametr není nastavena žádná hodnota, je automatický restart počítače blokován. Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Restartování je vyžadováno pouze v případě, že je nutné před instalací odebrat nekompatibilní aplikace. Restartování může být také vyžadováno při aktualizaci verze aplikace.
	`AddEnvironment`	Do systémové proměnné %PATH% přidejte cestu ke spustitelným souborům, které se nachází v instalační složce aplikace Kaspersky Endpoint Security. Dostupné hodnoty: • `1` – systémová proměnná %PATH% je doplněna o cestu ke spustitelným souborům, které se nachází v instalační složce aplikace Kaspersky Endpoint Security. • `0` – systémová proměnná %PATH% není doplněna o cestu ke spustitelným souborům, které se nachází v instalační složce aplikace Kaspersky Endpoint Security.
	`AMPPL`	Povolí nebo zakáže ochranu procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL (Antimalware Protected Process Light). Podrobnější informace o fungování technologie AM-PPL najdete na webu společnosti Microsoft. Technologie AM-PPL je k dispozici pro operační systémy Windows 10 verze 1703 (RS2) nebo novější a pro operační systémy Windows Server 2019. Dostupné hodnoty: • `1` – je povolena ochrana procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL. • `0` – je zakázána ochrana procesů služby Kaspersky Endpoint Security pomocí technologie AM-PPL.
	`SetupReg`	Povolí zápis klíčů registru ze souboru setup.reg do registru. Hodnota parametru `SetupReg: setup.reg`.
	`EnableTraces`	Povolí nebo zakáže trasování aplikací. Po spuštění uloží aplikace Kaspersky Endpoint Security soubory trasování do složky %ProgramData%/Kaspersky Lab\KES\Traces. Dostupné hodnoty: • `1` – je povoleno trasování aplikací.

		• `0` – je zakázáno trasování aplikací (výchozí hodnota).
	`TracesLevel`	Úroveň podrobností trasování. Dostupné hodnoty: • `100` (kritické). Pouze zprávy o závažných chybách. • `200` (vysoké). Zprávy o všech chybách, včetně závažných chyb. • `300` (diagnostické). Zprávy o všech chybách a varováních. • `400` (důležité). Všechny chybové zprávy, varování a další informace. • `500` (normální). Zprávy o všech chybách a varováních a podrobné informace o provozu aplikace v normálním režimu (výchozí). • `600` (nízké). Všechny zprávy.
	`RESTAPI`	Správa aplikace prostřednictvím rozhraní REST API. Chcete-li spravovat aplikaci pomocí rozhraní REST API, musíte zadat uživatelské jméno (parametr `RESTAPI_User`). Dostupné hodnoty: • `1` – správa přes REST API je povolena. • `0` – správa přes REST API je blokována (výchozí hodnota). Chcete-li spravovat aplikaci pomocí rozhraní REST API, musí být povolena správa pomocí administrativních systémů. To provedete nastavením parametru `AdminKitConnector=1`. Pokud spravujete aplikaci pomocí REST API, není možné spravovat aplikaci pomocí systémů pro správu společnosti Kaspersky.
	`RESTAPI_User`	Uživatelské jméno účtu domény systému Windows použitého pro správu aplikace prostřednictvím rozhraní REST API. Správa aplikace prostřednictvím rozhraní REST API je k dispozici pouze pro tohoto uživatele. Zadejte uživatelské jméno ve formátu `<DOMAIN>\<UserName>` (například `RESTAPI_User=COMPANY\Administrator`). Pro práci s rozhraním REST API můžete vybrat pouze jednoho uživatele. Předpokladem pro správu aplikace prostřednictvím rozhraní REST API je přidání uživatelského jména.
	`RESTAPI_Port`	Port používaný pro správu aplikace prostřednictvím rozhraní REST API. Ve výchozím nastavení je použit port 6782.
`[Components]`	`ALL`	Instalace všech součástí. Pokud je zadána hodnota parametru `1`, nainstalují se všechny součásti bez ohledu na nastavení instalace pro jednotlivé součásti.

	`MailThreatProtection`	Ochrana před hrozbami v poště
	`WebThreatProtection`	Ochrana před webovými hrozbami
	`AMSI`	Ochrana AMSI
	`HostIntrusionPrevention`	Prevence narušení hostitele
	`BehaviorDetection`	Detekce chování
	`ExploitPrevention`	Prevence zneužití
	`RemediationEngine`	Modul pro nápravu
	`Brána firewall`	Brána firewall
	`NetworkThreatProtection`	Ochrana před síťovými hrozbami
	`WebControl`	Kontrola webu;
	`DeviceControl`	Kontrola zařízení;
	`ApplicationControl`	Kontrola aplikací;
	`AdaptiveAnomaliesControl`	Adaptivní kontrola anomálií.
	`FileEncryption`	Knihovny šifrování na úrovni souborů.
	`DiskEncryption`	Knihovny úplného šifrování disku.
	`BadUSBAttackPrevention`	Ochrana před útoky BadUSB
	`AntiAPT`	Endpoint Agent. *Endpoint Agent* nainstaluje aplikaci Kaspersky Endpoint Agent 3.10 pro interakci mezi aplikací a řešeními společnosti Kaspersky pro detekci pokročilých hrozeb (například Kaspersky Sandbox).
	`AdminKitConnector`	Správa aplikací pomocí systémů pro správu. Mezi systémy pro správu patří například Kaspersky Security Center. Kromě systémů pro správu společnosti Kaspersky můžete také používat řešení třetích stran. Aplikace Kaspersky Endpoint Security poskytuje k těmto účelům rozhraní API. Dostupné hodnoty: • `1` – správa aplikací je povolena pomocí systémů pro správu (výchozí hodnota). • `0` – správa aplikací je povolena pouze prostřednictvím lokálního rozhraní.
`[Tasks]`	`ScanMyComputer`	Úloha Úplná kontrola. Dostupné hodnoty: • `1` – úloha je přidána na seznam úloh aplikace Kaspersky Endpoint Security. • `0` – úloha není přidána na seznam úloh aplikace Kaspersky Endpoint Security.
	`ScanCritical`	Úloha Kontrola kritických oblastí. Dostupné hodnoty: • `1` – úloha je přidána na seznam úloh aplikace Kaspersky Endpoint Security.

		• `0` – úloha není přidána na seznam úloh aplikace Kaspersky Endpoint Security.
	`Updater`	Úloha Aktualizace. Dostupné hodnoty: • `1` – úloha je přidána na seznam úloh aplikace Kaspersky Endpoint Security. • `0` – úloha není přidána na seznam úloh aplikace Kaspersky Endpoint Security.

Změnit součásti aplikace

Během instalace aplikace můžete vybrat součásti, které budou k dispozici. Dostupné součásti aplikace můžete změnit následujícími způsoby:

- Místně pomocí průvodce instalací.

  Součásti aplikace lze měnit způsobem obvyklým pro operační systém Windows, což je v části Ovládací panely. Spusťte průvodce nastavením aplikace a vyberte možnost pro změnu dostupných součástí aplikace. Postupujte podle pokynů na obrazovce.

- Vzdáleně prostřednictvím aplikace Kaspersky Security Center.

  Úloha *Změnit součásti aplikace* vám umožňuje změnit součásti aplikace Kaspersky Endpoint Security po nainstalování aplikace.

Při změně součástí aplikace vezměte v úvahu následující zvláštní aspekty:

- V počítačích se systémem Windows Server nelze nainstalovat všechny součásti aplikace Kaspersky Endpoint Security (není k dispozici například součást Adaptivní kontrola anomálií).
- Pokud jsou pevné disky v počítači chráněny úplným šifrováním disku (FDE), nemůžete odebrat součást Úplné šifrování disku. Chcete-li součást Úplné šifrování disku odebrat, dešifrujte všechny pevné disky počítače.
- Pokud počítač obsahuje šifrované soubory (FLE) nebo pokud uživatel používá šifrované vyměnitelné jednotky (FDE nebo FLE), nebude možné po odebrání součástí šifrování dat získat přístup k souborům a vyměnitelným jednotkám. K souborům a vyměnitelným jednotkám můžete přistupovat přeinstalováním součástí šifrování dat.

Jak přidat nebo odebrat součásti aplikace v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnosti **Kaspersky Endpoint Security pro systém Windows (11.6.0)** → **Změnit součásti aplikace**.

Krok 2. Nastavení úlohy pro změnu součástí aplikace

Vyberte součásti aplikace, které budou k dispozici v počítači uživatele.

Zaškrtněte políčko **Odebrat nekompatibilní aplikace třetích stran**. Seznam nekompatibilních aplikací lze zobrazit v souboru `incompatible.txt`, který je součástí distribuční sady. Pokud jsou v počítači nainstalovány nekompatibilní aplikace, instalace aplikace Kaspersky Endpoint Security skončí chybou.

V případě potřeby povolte ochranu heslem při provádění úloh:

1. Klikněte na tlačítko **Další**.
2. Zaškrtněte políčko **Použijte heslo pro úpravu sady součástí aplikace**.
3. Zadejte přihlašovací údaje uživatelského účtu KLAdmin.

Krok 3. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 4. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně, nebo když je počítač nečinný.

Krok 5. Definování názvu úlohy

Zadejte název úlohy, například `Přidání součásti Kontrola aplikací`.

Krok 6. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Poté se změní sada součástí aplikace Kaspersky Endpoint Security v počítačích uživatelů v bezobslužném režimu. Nastavení dostupných součástí budou zobrazena v místním rozhraní aplikace. Součásti, které nebyly zahrnuty v aplikaci, jsou zakázány a nastavení těchto součástí nejsou k dispozici.

[Jak přidat nebo odebrat součásti aplikace ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.
2. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Změnit součásti aplikace**.
3. V poli **Název úlohy** zadejte krátký popis, například `Přidání součásti Kontrola aplikací`.
4. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

Krok 2. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. Například vyberte samostatnou skupinu pro správu nebo vytvořte výběr.

Krok 3. Dokončení vytvoření úlohy

Zaškrtněte políčko **Otevřít okno vlastností úlohy po vytvoření úlohy** a dokončete průvodce. Ve vlastnostech úlohy vyberte kartu **Nastavení aplikace** a vyberte součásti aplikace, které budou k dispozici.

V případě potřeby povolte ochranu heslem při provádění úloh:

1. V části **Rozšířené nastavení** zaškrtněte políčko **Použijte heslo pro úpravu sady součástí aplikace**.
2. Zadejte přihlašovací údaje uživatelského účtu KLAdmin.

Uložte změny a spusťte úlohu.

Poté se změní sada součástí aplikace Kaspersky Endpoint Security v počítačích uživatelů v bezobslužném režimu. Nastavení dostupných součástí budou zobrazena v místním rozhraní aplikace. Součásti, které nebyly zahrnuty v aplikaci, jsou zakázány a nastavení těchto součástí nejsou k dispozici.

Upgradování z předchozí verze aplikace

Při aktualizaci předchozí verze aplikace na novější verzi zvažte následující:

- Aplikace Kaspersky Endpoint Security 11.6.0 je kompatibilní s aplikací Kaspersky Security Center 12.

- Před zahájením aktualizace doporučujeme ukončit všechny aktivní aplikace.
- Pokud má počítač pevné disky, které jsou šifrovány pomocí úplného šifrování disku (FDE), musíte před upgradem aplikace Kaspersky Endpoint Security z verze 10 na verzi 11.0.0 nebo novější dešifrovat všechny šifrované pevné disky.

  Před aktualizací blokuje aplikace Kaspersky Endpoint Security funkci úplného šifrování disku. Pokud nelze funkci Úplné šifrování disku zamknout, instalace upgradu se nespustí. Po aktualizaci aplikace bude funkce úplného šifrování disku obnovena.

Aplikace Kaspersky Endpoint Security podporuje aktualizace u následujících verzí aplikace:

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 4 pro systém Windows (sestavení 10.2.6.3733).
- Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows (sestavení 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 1 pro systém Windows (sestavení 10.3.0.6294).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 2 pro systém Windows (sestavení 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 pro systém Windows (sestavení 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 pro systém Windows (sestavení 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 pro systém Windows (sestavení 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 pro systém Windows (sestavení 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 pro systém Windows SF1 (sestavení 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 pro systém Windows (sestavení 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 pro systém Windows (sestavení 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 pro systém Windows (sestavení 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 pro systém Windows CF1 (sestavení 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 pro systém Windows (sestavení 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 pro systém Windows (sestavení 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 pro systém Windows (sestavení 11.5.0.590).

Při upgradu aplikace Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows na verzi Kaspersky Endpoint Security 11.6.0 pro systém Windows budou soubory, které byly v předchozí verzi aplikace umístěny v záloze nebo karanténě, přesunuty v nové verzi aplikace do zálohy. Ve verzích starších než Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows nejsou soubory, které byly v předchozí verzi aplikace umístěny do zálohy a karantény, přeneseny do novější verze.

Aplikaci Kaspersky Endpoint Security lze v počítači aktualizovat několika způsoby:

- místně pomocí průvodce instalací,
- místně z příkazového řádku,
- vzdáleně prostřednictvím aplikace Kaspersky Security Center 12,
- vzdáleně prostřednictvím editoru správy zásad skupiny v systému Microsoft Windows (další podrobnosti viz *web technické podpory společnosti Microsoft*),
- vzdáleně pomocí aplikace System Center Configuration Manager.

Pokud je aplikace, která je nasazena v podnikové síti, vybavena jinou sadou součástí, než je výchozí sada, aktualizace aplikace prostřednictvím konzoly pro správu (MMC) se liší od aktualizace aplikace prostřednictvím webové konzoly a cloudové konzoly. Při aktualizaci aplikace Kaspersky Endpoint Security zvažte následující:

- Webová konzola aplikace Kaspersky Security Center nebo cloudová konzola aplikace Kaspersky Security Center.

  Pokud jste vytvořili instalační balíček pro novou verzi aplikace s výchozí sadou součástí, tato sada součástí se v počítači uživatele nezmění. Chcete-li používat aplikaci Kaspersky Endpoint Security s výchozí sadou součástí, musíte otevřít vlastnosti instalačního balíčku, změnit sadu součástí, vrátit se k původní sadě součástí a uložit změny.

- Konzola pro správu aplikace Kaspersky Security Center.

  Sada součástí aplikace po aktualizaci bude odpovídat sadě součástí v instalačním balíčku. To znamená, že pokud nová verze aplikace obsahuje výchozí sadu součástí, bude například z počítače odebrána Ochrana před útoky BadUSB, protože tato součást není ve výchozí sadě obsažena. Chcete-li pokračovat v používání aplikace se stejnou sadou součástí jako před aktualizací, vyberte požadované součásti v nastavení instalačního balíčku.

Odebrat aplikaci

Při odebrání aplikace Kaspersky Endpoint Security nebudou počítač a uživatelská data chráněné před hrozbami.

Aplikaci Kaspersky Endpoint Security lze z počítače odinstalovat několika způsoby:

- místně pomocí průvodce instalací,
- místně z příkazového řádku,
- vzdáleně pomocí sady softwaru Kaspersky Security Center (další informace najdete *v nápovědě k sadě Kaspersky Security Center*),
- vzdáleně prostřednictvím editoru správy zásad skupiny v systému Microsoft Windows (další podrobnosti viz *web technické podpory společnosti Microsoft*),

Pokud jste během instalace aplikace vybrali součást Endpoint Agent, do počítače se nainstalují následující dvě aplikace: Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Po odinstalování aplikace Kaspersky Endpoint Security bude automaticky odinstalována i součást Kaspersky Endpoint Agent.

Odinstalace prostřednictvím aplikace Kaspersky Security Center

Aplikaci můžete vzdáleně odinstalovat pomocí úlohy *vzdálené odinstalace aplikace*. Při provádění úlohy stáhne aplikace Kaspersky Endpoint Security nástroj pro odinstalaci aplikace do počítače uživatele. Po dokončení odinstalace aplikace bude nástroj automaticky odstraněn.

Jak odebrat aplikaci pomocí konzoly pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte položky **Server pro správu Kaspersky Security Center** → **Další** → **Vzdálená odinstalace aplikace**.

Krok 2. Výběr aplikace, která má být odebrána

Vyberte možnost **Odinstalovat aplikaci podporovanou aplikací Kaspersky Security Center**.

Krok 3. Nastavení úlohy pro odinstalování aplikace

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

Krok 4. Odinstalace nastavení nástroje

Nakonfigurujte následující další nastavení aplikace:

- **Vynucovat stažení nástroje odinstalace**. Vyberte způsob doručení nástroje:
  - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Aplikace Kaspersky Endpoint Security je odinstalována pomocí nástrojů součásti Network Agent.
  - **Použití prostředků systému Microsoft Windows prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému prostřednictvím serveru pro správu. Tuto možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.
  - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Nástroj je do klientských počítačů doručen prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.
- **Před stažením ověřte verzi operačního systému**. V případě potřeby zrušte zaškrtnutí tohoto políčka. To umožňuje zabránit stažení nástroje pro odinstalaci aplikace, pokud operační systém počítače nesplňuje požadavky na software. Pokud si jste jisti, že operační systém počítače splňuje požadavky na software, můžete toto ověřování přeskočit.

Pokud je operace odinstalování aplikace chráněna heslem, postupujte takto:

1. Zaškrtněte políčko **Při odinstalaci použít heslo**.
2. Klikněte na tlačítko **Upravit**.

3. Zadejte heslo k účtu KLAdmin.

Krok 5. Výběr nastavení restartování operačního systému

Po odinstalování aplikace je nutné restartovat počítač. Vyberte akci, která bude provedena pro restart počítače.

Krok 6. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 7. Výběr účtu pro spuštění úlohy

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Jestliže provádíte odinstalaci aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 8. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně, nebo když je počítač nečinný.

Krok 9. Definování názvu úlohy

Zadejte název úlohy, například `Odinstalace Kaspersky Endpoint Security 11.6.0`

Krok 10. Vytvoření úloh po dokončení

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Aplikace bude odinstalována v bezobslužném režimu.

[Jak odebrat aplikaci prostřednictvím webové konzoly a cloudové konzoly](#)

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Aplikace** vyberte možnost **Kaspersky Security Center**.
2. V rozevíracím seznamu **Typ úlohy** vyberte možnost **vzdálené odinstalace aplikace**.
3. Do pole **Název úlohy** zadejte krátký popis, například `Odinstalace aplikace Kaspersky Endpoint Security z počítačů technické podpory`.
4. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

Krok 2. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. Například vyberte samostatnou skupinu pro správu nebo vytvořte výběr.

Krok 3. Konfigurace nastavení odinstalace aplikace

V tomto kroku nakonfigurujte nastavení odinstalace aplikace:

1. Vyberte možnost **Odebrat spravovanou aplikaci**.
2. Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.
3. **Vynucovat stažení nástroje odinstalace**. Vyberte způsob doručení nástroje:

   - **Pomocí součásti Network Agent**. Pokud není v počítači nainstalována součást Network Agent, první součást Network Agent bude nainstalována pomocí nástrojů operačního systému. Aplikace Kaspersky Endpoint Security je odinstalována pomocí nástrojů součásti Network Agent.
   - **Použití prostředků systému Microsoft Windows prostřednictvím serveru pro správu**. Soubory budou do klientských počítačů doručeny pomocí prostředků operačního systému prostřednictvím serveru pro správu. Tuto možnost můžete vybrat, pokud v klientském počítači není nainstalována součást Network Agent, ale klientský počítač je ve stejné síti jako server pro správu.
   - **Pomocí prostředků operačního systému prostřednictvím distribučních bodů**. Nástroj je do klientských počítačů doručen prostředky operačního systému prostřednictvím distribučních bodů. Tuto možnost můžete vybrat, pokud je v síti alespoň jeden distribuční bod. Další informace o distribučních bodech *najdete v nápovědě k aplikaci Kaspersky Security Center*.

4. V části **Maximální počet souběžných stažení** nastavte limit počtu požadavků o stažení nástroje pro odinstalaci aplikace zasílaných na server pro správu. Limit počtu požadavků pomůže zabránit přetížení sítě.

5. V poli **Počet pokusů o odinstalaci** nastavte limit počtu pokusů o odinstalaci aplikace. Pokud odinstalace aplikace Kaspersky Endpoint Security skončí chybou, úloha automaticky spustí odinstalaci znovu.

6. V případě potřeby zrušte zaškrtnutí políčka **Check the operating system version before installation**. To umožňuje zabránit stažení nástroje pro odinstalaci aplikace, pokud operační systém počítače nesplňuje požadavky na software. Pokud si jste jisti, že operační systém počítače splňuje požadavky na software, můžete toto ověřování přeskočit.

Krok 4. Výběr účtu pro spuštění úlohy

Vyberte účet pro instalaci součásti Network Agent pomocí nástrojů operačního systému. V tomto případě jsou pro přístup k počítači vyžadována oprávnění správce. Můžete přidat více účtů. Pokud účet nemá dostatečná oprávnění, průvodce instalací použije další účet. Jestliže provádíte odinstalaci aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent, není nutné vybírat účet.

Krok 5. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Dokončit** dokončete průvodce. V seznamu úloh se zobrazí nová úloha.

Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**. Aplikace bude odinstalována v bezobslužném režimu. Po dokončení odinstalace zobrazí aplikace Kaspersky Endpoint Security výzvu k restartování počítače.

Pokud je operace odinstalace aplikace chráněná heslem, zadejte ve vlastnostech úlohy *vzdálené odinstalace aplikace* heslo k účtu KLAdmin. Bez hesla nebude úloha provedena.

Použití hesla k účtu KLAdmin v úloze vzdálené odinstalace aplikace:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **vzdálené odinstalace aplikace** Kaspersky Security Center.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Nastavení aplikace**.

4. Zaškrtněte políčko **Při odinstalaci použít heslo**.

5. Zadejte heslo k účtu KLAdmin.

6. Klikněte na tlačítko **Uložit**.

Odinstalace aplikace pomocí průvodce

Aplikaci Kaspersky Endpoint Security lze odebrat obvyklou metodou pro operační systém Windows, což je v části Ovládací panely. Spustí se Průvodce instalací. Postupujte podle pokynů na obrazovce.

Během další instalace aplikace (například při přechodu na novější verzi aplikace) můžete určit, která z dat, která aplikace používá, chcete uložit pro budoucí použití. Pokud žádná data neurčíte, aplikace bude odstraněna úplně.

Uložit můžete následující data:

- **Aktivační data**, díky nimž nebudete muset aplikaci znovu aktivovat. Pokud před instalací neskončila platnost licenčního období, aplikace Kaspersky Endpoint Security automaticky přidá licenční klíč.
- **Soubory zálohy** – soubory, které byly aplikací zkontrolovány a uloženy do zálohy.

  Soubory zálohy, které zůstanou uloženy po odebrání aplikace, mohou být použity pouze stejnou verzí aplikace, jaká byla použita k jejich vytvoření.

  Pokud plánujete objekty zálohy použít po odstranění aplikace, je nutné je obnovit před odebráním aplikace. Odborníci společnosti Kaspersky však obnovení objektů ze zálohy nedoporučují, protože by mohly být pro počítač škodlivé.

- **Operační nastavení aplikace** – hodnoty nastavení aplikace, které byly zvoleny při konfiguraci aplikace.
- **Místní úložiště šifrovacích klíčů** – data poskytující přístup k souborům a jednotkám, které byly zašifrovány před odstraněním aplikace. Chcete-li zajistit přístup k šifrovaným souborům a jednotkám, při přeinstalování aplikace Kaspersky Endpoint Security musíte vybrat funkci šifrování dat. Pro přístup k dříve zašifrovaným souborům a jednotkám není nutná žádná další akce.

Odebrání aplikace z příkazového řádku

Aplikaci Kaspersky Endpoint Security lze odinstalovat z příkazového řádku jedním z těchto způsobů:

- V interaktivním režimu za použití průvodce instalací aplikace.
- V bezobslužném režimu. Po spuštění odinstalace v bezobslužném režimu nemusíte během odebírání provádět žádnou činnost. Chcete-li odinstalovat aplikaci v bezobslužném režimu, použijte přepínače `/s` a `/qn`.

Odinstalace aplikace v bezobslužném režimu:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, kde se nachází distribuční balíček aplikace Kaspersky Endpoint Security.
3. Spusťte následující příkaz:

   - Pokud proces odebrání není chráněn heslem:

     ```
     setup_kes.exe /s /x
     ```

     nebo

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` je jedinečný identifikátor aplikace. GUID aplikace můžete zjistit pomocí následujícího příkazu:

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

   - Pokud je proces odebrání chráněn heslem:

     ```
     setup_kes.exe /pKLLOGIN=<uživatelské jméno> /pKLPASSWD=<heslo> /s /x
     ```

nebo

```
msiexec.exe /x <GUID> KLLOGIN=<uživatelské jméno> KLPASSWD=<heslo> /qn
```

Příklad:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

Poskytování licence na aplikaci

Tato část poskytuje informace o obecných konceptech souvisejících s licencováním aplikace.

O licenční smlouvě s koncovým uživatelem (EULA)

Licenční smlouva s koncovým uživatelem je závazná smlouva mezi vámi a společností AO Kaspersky Lab, která stanovuje podmínky, za kterých můžete tuto aplikaci používat.

Doporučujeme vám, abyste si pečlivě přečetli podmínky této licenční smlouvy ještě před použitím aplikace.

Podmínky licenční smlouvy můžete zobrazit následujícími způsoby:

- Při instalaci aplikace Kaspersky Endpoint Security v interaktivním režimu.
- Přečtením souboru license.txt. Tento dokument je součástí distribučního balíčku aplikace a je také umístěn v instalační složce aplikace `%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\<národní_prostředí>\KES`.

Potvrzením souhlasu s licenční smlouvou s koncovým uživatelem při instalaci aplikace přijímáte podmínky licenční smlouvy s koncovým uživatelem. Pokud podmínky licenční smlouvy s koncovým uživatelem nepřijmete, musíte instalaci zrušit.

O licenci

Licence je časově omezené právo k používání aplikace, jež se uděluje na základě licenční smlouvy s koncovým uživatelem.

Platná licence vám poskytuje nárok využívat následující druhy služeb:

- Použití aplikace v souladu s podmínkami licenční smlouvy s koncovým uživatelem
- Technická podpora

Rozsah podmínek využití služeb a aplikace je závislý na typu licence, na jejímž základě je aplikace aktivována.

Jsou poskytovány následující typy licence:

- *Zkušební* – bezplatná licence určená k vyzkoušení aplikace.

  Zkušební licence je obvykle krátkodobá. Když platnost zkušební licence skončí, všechny funkce aplikace Kaspersky Endpoint Security se zakážou. Budete-li chtít pokračovat v používání aplikace, je nutné zakoupit komerční licenci.

  Aplikaci můžete aktivovat na základě zkušební licence pouze jednou.

- *Komerční* – placená licence, která je poskytována při zakoupení aplikace Kaspersky Endpoint Security.

  Funkce aplikace dostupné na základě komerční licence jsou závislé na výběru produktu. Vybraný produkt je uveden v položce Licenční certifikát. Informace o dostupných produktech můžete najít na webu společnosti Kaspersky.

Po vypršení platnosti komerční licence se klíčové funkce aplikace deaktivují. Budete-li chtít pokračovat v používání aplikace, je nutné si obnovit komerční licenci. Pokud obnovení licence neplánujete, musíte aplikaci z počítače odstranit.

O licenčním certifikátu

Licenční certifikát je dokument, který je přenesen na uživatele společně se souborem klíče nebo aktivačním kódem.

Licenční certifikát obsahuje následující informace o licenci:

- Licenční klíč nebo číslo objednávky.
- Podrobnosti o uživateli, kterému je licence udělena.
- Podrobnosti o aplikaci, kterou lze pomocí licence aktivovat.
- Omezení počtu licencovaných jednotek (například počtu zařízení, ve kterých lze aplikaci na základě licence používat).
- Datum počátku licenčního období.
- Datum vypršení platnosti licence nebo licenční období.
- Typ licence.

O předplatném

Předplatné aplikace Kaspersky Endpoint Security představuje nákupní objednávku aplikace s konkrétními parametry (například datum vypršení platnosti a počet chráněných zařízení). Předplatné aplikace Kaspersky Endpoint Security si můžete objednat u svého poskytovatele služeb (například poskytovatele připojení k internetu). Předplatné lze obnovit ručně nebo automaticky a můžete ho také zrušit. Své předplatné můžete spravovat na webových stránkách poskytovatele služeb.

Předplatné může být omezené (například na dobu jednoho roku) nebo neomezené (bez data vypršení platnosti). Aby aplikace Kaspersky Endpoint Security fungovala po skončení období omezeného předplatného, musíte předplatné obnovit. Neomezené předplatné se obnovuje automaticky, pokud jsou služby dodavatele včas předplaceny.

V případě vypršení platnosti omezeného předplatného vám může být poskytnuta lhůta pro obnovení předplatného, během které aplikace nadále funguje. O dostupnosti a době trvání této lhůty rozhoduje poskytovatel služeb.

Abyste mohli aplikaci Kaspersky Endpoint Security používat v rámci předplatného, musíte použít aktivační kód od poskytovatele služeb. Po použití aktivačního kódu se přidá aktivní klíč. Aktivní klíč určuje licenci pro používání aplikace v rámci předplatného. V rámci předplatného není možné přidat rezervní licenční klíč.

Aktivační kódy zakoupené v rámci předplatného nelze použít k aktivaci dřívějších verzí aplikace Kaspersky Endpoint Security.

O licenčním klíči

Licenční klíč je posloupnost bitů, kterou můžete použít k aktivaci a následnému použití aplikace v souladu s podmínkami licenční smlouvy s koncovým uživatelem.

Certifikát licence není poskytován pro klíč přidaný v rámci předplatného.

Licenční klíč můžete do aplikace přidat přidáním souboru klíče nebo zadáním aktivačního kódu.

Při porušení podmínek licenční smlouvy s koncovým uživatelem může být klíč společností Kaspersky zablokován. Pokud byl klíč zablokován, je třeba přidat jiný klíč, jinak nebude možné aplikaci nadále používat.

Existují dva typy klíče: aktivní a další rezervní.

Aktivní klíč je klíč, který je v aplikaci aktuálně používán. Jako aktivní klíč je možné přidat klíč zkušební licence nebo komerční licence. Aplikace nemůže mít více aktivních klíčů současně.

Rezervní klíč je klíč opravňující uživatele k použití aplikace, který však není aktuálně používaný. Po skončení platnosti aktivního klíče se automaticky aktivuje rezervní klíč. Rezervní klíč lze přidat jen v případě, když je k dispozici aktivní klíč.

Klíč pro zkušební licenci lze přidat jen jako aktivní klíč. Nelze jej přidat jako rezervní klíč. Klíč zkušební licence nemůže nahradit aktivní klíč pro komerční licenci.

Pokud je klíč přidán do seznamu zakázaných klíčů, funkce aplikace definované licencí použitou k aktivaci aplikace zůstanou k dispozici po dobu osmi dnů. Aplikace upozorní uživatele, že klíč byl přidán do seznamu zakázaných klíčů. Po osmi dnech se funkčnost aplikace omezí na úroveň funkčnosti, která je k dispozici po vypršení licence. Můžete používat součásti ochrany a kontroly a spustit kontrolu s využitím databází aplikace, které byly nainstalovány před vypršením platnosti licence. Aplikace také dále šifruje soubory, které byly změněny a zašifrovány před vypršením platnosti licence, ale nešifruje nové soubory. Použití služby Kaspersky Security Network není k dispozici.

O aktivačním kódu

Aktivační kód je jedinečná sekvence 20 alfanumerických znaků. Zadáním aktivačního kódu přidáte licenční klíč, který aktivuje aplikaci Kaspersky Endpoint Security. Po zakoupení aplikace Kaspersky Endpoint Security obdržíte aktivační kód na e-mailovou adresu, kterou jste zadali.

Při aktivaci aplikace pomocí aktivačního kódu je vyžadován přístup k internetu pro připojení k aktivačním serverům Kaspersky.

Když aplikaci aktivujete aktivačním kódem, přidá se aktivní klíč. Rezervní licenční klíč lze přidat pouze pomocí aktivačního kódu a nelze jej přidat pomocí souboru klíče.

Pokud po aktivaci aplikace ztratíte aktivační kód, můžete jej obnovit. Aktivační kód můžete potřebovat například k registraci služby Kaspersky CompanyAccount. Pokud došlo po aktivaci aplikace ke ztrátě aktivačního kódu, kontaktujte partnera společnosti Kaspersky, u kterého jste licenci zakoupili.

O souboru klíče

Soubor klíče je soubor s příponou .key, který obdržíte od společnosti Kaspersky. Tento soubor klíče slouží k přidání licenčního klíče, který aplikaci aktivuje.

Na e-mailovou adresu, kterou jste zadali při zakoupení aplikace Kaspersky Endpoint Security nebo při objednání zkušební verze aplikace Kaspersky Endpoint Security, obdržíte soubor s klíči.

K aktivaci aplikace pomocí souboru klíče není třeba se připojovat k aktivačním serverům společnosti Kaspersky.

Omylem odstraněný soubor klíče můžete obnovit. Soubor klíče můžete potřebovat například k registraci služby Kaspersky CompanyAccount.

Při obnově souboru klíče proveďte jednu z následujících akcí:

- Kontaktujte prodejce licence.
- Získejte soubor klíče na webových stránkách společnosti Kaspersky na základně svého stávajícího aktivačního kódu.

Když aplikaci aktivujete souborem klíče, přidá se aktivní klíč. Rezervní licenční klíč lze přidat pouze pomocí souboru klíče a nelze jej přidat pomocí aktivačního kódu.

Aktivace aplikace

Aktivace je proces aktivace licence, která umožňuje používat plně funkční verzi aplikace až do skončení platnosti licence. Aktivace aplikace zahrnuje přidání licenčního klíče.

Aplikaci lze aktivovat jedním z následujících způsobů:

- Místně z rozhraní aplikace za použití průvodce aktivací. Tímto způsobem můžete přidat aktivní klíč a rezervní klíč.
- Vzdáleně pomocí sady softwaru Kaspersky Security Center, a to vytvořením a následným spuštěním úlohy přidání licenčního klíče. Tímto způsobem můžete přidat aktivní klíč a rezervní klíč.
- Vzdáleně distribuováním souborů klíčů a aktivačních kódů uložených v úložišti klíčů serveru pro správu aplikace Kaspersky Security Center do klientských počítačů. Další informace o distribuci klíčů najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*. Tímto způsobem můžete přidat aktivní klíč a rezervní klíč.

  Nejprve je distribuován aktivační kód zakoupený v rámci předplatného.

- Pomocí příkazového řádku.

Aktivace aplikace pomocí aktivačního kódu může chvíli trvat (během vzdálené nebo neinteraktivní instalace). Doba je závislá na rozložení zatížení v rámci aktivačních serverů společnosti Kaspersky. Pokud potřebujete aplikaci aktivovat ihned, můžete proces aktivace přerušit a aktivaci provést pomocí průvodce aktivací.

Aktivace prostřednictvím aplikace Kaspersky Security Center

Aplikaci můžete aktivovat vzdáleně prostřednictvím aplikace Kaspersky Security Center následujícími způsoby:

- Pomocí úlohy *Přidat klíč*.

  Tento způsob umožňuje přidat klíč do konkrétního počítače nebo počítačů, které jsou součástí skupiny pro správu.

- Distribucí klíče, který je uložen na serveru pro správu aplikace Kaspersky Security Center, do počítačů.

  Tento způsob umožňuje automaticky přidat klíč do počítačů, které jsou již připojeny k aplikaci Kaspersky Security Center, a do nových počítačů. Chcete-li použít tento způsob, musíte nejdříve přidat klíč na server pro správu aplikace Kaspersky Security Center. Podrobnosti o přidání klíčů na server pro správu aplikace Kaspersky Security Center najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

Pro cloudovou konzolu Kaspersky Security Center je poskytována zkušební verze. *Zkušební verze* je speciální verze cloudové konzoly aplikace Kaspersky Security Center, která má uživatele seznámit s funkcemi aplikace. V této verzi můžete provádět akce v pracovním prostoru po dobu 30 dnů. Všechny spravované aplikace jsou automaticky spouštěny na základě zkušební licence pro cloudovou konzolu aplikace Kaspersky Security Center, včetně aplikace Kaspersky Endpoint Security. Po vypršení zkušební licence ke cloudové konzole Kaspersky Security Center ale nemůžete aktivovat aplikaci Kaspersky Endpoint Security pomocí vlastní zkušební licence. Podrobné informace o správě licencí aplikace Kaspersky Security Center *najdete v nápovědě ke cloudové konzole aplikace Kaspersky Security Center*.

Zkušební verze cloudové konzoly aplikace Kaspersky Security Center neumožňuje následné přepnutí na komerční verzi. Po uplynutí 30denního období bude jakýkoli zkušební pracovní prostor s veškerým obsahem automaticky odstraněn.

Použití licencí můžete sledovat následujícími způsoby:

- Zobrazte možnost *Key usage report* pro infrastrukturu organizace (**Monitoring and reports** → **Reports**).
- Zobrazte stavy počítačů na kartě **Devices** → **Managed devices**. Pokud aplikace není aktivována, počítač bude ve stavu ⚠ a stav bude mít popis **Aplikace není aktivována**.
- Zobrazte informace o licenci ve vlastnostech.
- Zobrazte vlastnosti klíče (**Operations** → **Licensing**).

Jak aktivovat aplikaci v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnosti **Kaspersky Endpoint Security pro systém Windows (11.6.0)** → **Přidat klíč**.

Krok 2. Přidání klíče

Zadejte aktivační kód nebo vyberte soubor klíče.

Podrobnosti o přidání klíčů do úložiště aplikace Kaspersky Security Center *najdete v průvodci nápovědou k aplikaci Kaspersky Security Center*.

Krok 3. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 4. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně, nebo když je počítač nečinný.

Krok 5. Definování názvu úlohy

Zadejte název úlohy, například `Aktivace aplikace Kaspersky Endpoint Security pro systém Windows`.

Krok 6. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. Aplikace Kaspersky Endpoint Security bude poté aktivována v počítačích uživatelů v bezobslužném režimu.

[Jak aktivovat aplikaci ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.
2. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Přidat klíč**.
3. V poli **Název úlohy** zadejte krátký popis, například `Aktivace aplikace Kaspersky Endpoint Security pro systém Windows`.
4. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy. Klikněte na tlačítko **Další**.

Krok 2. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 3. Výběr licence

Vyberte licenci, kterou chcete použít k aktivaci aplikace. Klikněte na tlačítko **Další**.

Klíče můžete přidat do webové konzoly (**Operace** → **Správa licence**).

Krok 4. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Dokončit** dokončete průvodce. V seznamu úloh se zobrazí nová úloha. Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**. Aplikace Kaspersky Endpoint Security bude poté aktivována v počítačích uživatelů v bezobslužném režimu.

Ve vlastnostech úlohy *Přidat klíč* můžete do počítače přidat rezervní klíč. *Rezervní klíč* se aktivuje v případě vypršení platnosti nebo odstranění aktivního klíče. Dostupnost rezervního klíče vám umožní vyhnout se omezením funkcí aplikace v případě vypršení platnosti licence.

Jak automaticky přidat licenční klíč do počítačů pomocí konzoly pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Licence Kaspersky**.

   Otevře se seznam licenčních klíčů.

2. Otevřete vlastnosti licenčního klíče.

3. V části **Obecné** zaškrtněte políčko **Automaticky distribuovaný licenční klíč**.

4. Uložte změny.

   Klíč bude následně automaticky distribuován do příslušných počítačů. Během automatické distribuce klíče jako aktivního nebo rezervního klíče je zohledněn limit licencí pro počet počítačů (nastavený ve vlastnostech klíče). Pokud je dosaženo limitu licencí, distribuce tohoto klíče do počítačů se automaticky ukončí. V části **Zařízení** můžete zobrazit počet počítačů, do kterých byl přidán klíč, a další data ve vlastnostech klíče.

Jak automaticky přidat licenční klíč do počítačů pomocí webové konzoly a konzoly pro správu

1. V hlavním okně webové konzole vyberte možnost **Operace** → **Správa licence** → **Licence Kaspersky**.

   Otevře se seznam licenčních klíčů.

2. Otevřete vlastnosti licenčního klíče.

3. Na kartě **Obecné** zapněte přepínací tlačítko **Nasazovat klíč automaticky**.

4. Uložte změny.

   Klíč bude následně automaticky distribuován do příslušných počítačů. Během automatické distribuce klíče jako aktivního nebo rezervního klíče je zohledněn limit licencí pro počet počítačů (nastavený ve vlastnostech klíče). Pokud je dosaženo limitu licencí, distribuce tohoto klíče do počítačů se automaticky ukončí. Na kartě **Zařízení** můžete zobrazit počet počítačů, do kterých byl přidán klíč, a další data ve vlastnostech klíče.

Použití průvodce aktivací k aktivaci aplikace

Postup aktivace aplikace Kaspersky Endpoint Security pomocí průvodce aktivací:

1. Klikněte na tlačítko **Licence** v dolní části hlavního okna aplikace.

2. V okně, které se otevře, klikněte na tlačítko **Aktivovat aplikaci pomocí nové licence**.

Spustí se průvodce aktivací aplikace. Postupujte podle pokynů průvodce aktivací.

Aktivace aplikace z příkazového řádku

Chcete-li aplikaci aktivovat z příkazového řádku,

do příkazového řádku zadejte následující řetězec:

```
avp.com license /add <aktivační kód nebo soubor klíče> [/login=<uživatelské jméno>
/password=<heslo>]
```

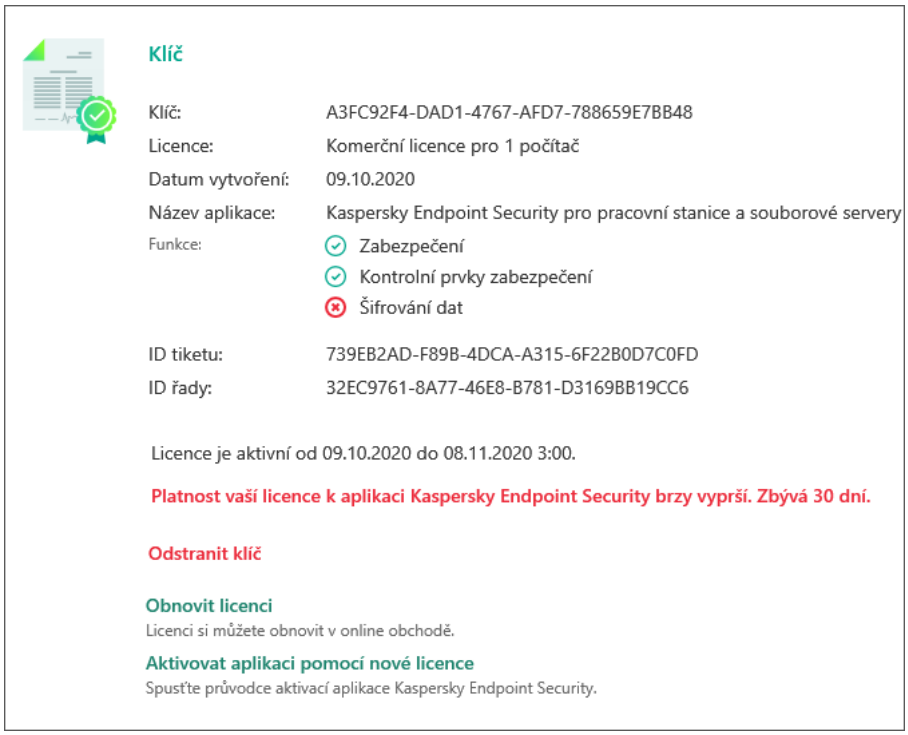
Pokud je aktivována ochrana heslem, musíte zadat přihlašovací údaje uživatelského účtu (`/login=<uživatelské jméno> /password=<hesla>`).

Zobrazení informací o licenci

Postup zobrazení informací o licenci:

Klikněte na tlačítko **Licence** nacházející se v dolní části hlavního okna aplikace.

Otevře se okno **Správa licence**. V tomto okně se zobrazí informace o licenci (viz obrázek níže).



Okno Správa licence

V okně **Správa licence** jsou uvedeny následující informace:

- **Stav klíče**. V počítači lze uložit několik klíčů. Existují dva typy klíče: aktivní a další rezervní. Aplikace nemůže mít více aktivních klíčů současně. Rezervní klíč může být aktivován pouze v případě, že skončí platnost aktivního klíče nebo že aktivní klíč odstraníte pomocí tlačítka .
- **Klíč**. *Klíč* je jedinečná alfanumerická série, která je vygenerována z aktivačního kódu nebo souboru klíče.
- **Licence**. K dispozici jsou následující typy licencí: zkušební a komerční.
- **Název aplikace**. Úplný název zakoupené aplikace společnosti Kaspersky.

- **Funkce**. Funkce aplikace, které jsou k dispozici v rámci vaší licence. Mezi funkce může patřit Ochrana, Kontrolní prvky zabezpečení, Šifrování dat a další. Seznam dostupných funkcí je rovněž uveden v licenčním certifikátu.
- **Další informace o licenci**. Typ licence, počet počítačů, na který se tato licence vztahuje, datum a čas začátku a vypršení platnosti licence (pouze pro aktivní klíč).

  Čas vypršení platnosti licence je zobrazen podle časového pásma nakonfigurovaného v operačním systému.

V okně Správa licence můžete také provést jednu z následujících akcí:

- **Zakoupit licenci** / **Obnovit licenci**. Otevře se webová stránka internetového obchodu společnosti Kaspersky, kde můžete zakoupit nebo obnovit licenci. Chcete-li to provést, zadejte informace o společnosti a zaplaťte objednávku.
- **Aktivujte aplikaci s novou licencí**. Spustí se průvodce aktivací aplikace. V tomto průvodci můžete přidat klíč pomocí aktivačního kódu nebo souboru klíče. Průvodce aktivací aplikace umožňuje přidat aktivní klíč a pouze jeden rezervní klíč.

Zakoupení licence

Po instalaci aplikace si můžete zakoupit licenci. Při zakoupení licence obdržíte aktivační kód nebo soubor klíče pro aktivaci aplikace.

Chcete-li získat licenci, postupujte takto:

1. V hlavním okně aplikace klikněte na tlačítko **Licence**.
2. V okně **Správa licence** proveďte jednu z následujících akcí:
   - Pokud nebyly přidány žádné klíče nebo byl přidán klíč zkušební licence, klikněte na tlačítko **Zakoupit licenci**.
   - Pokud je přidáván klíč pro komerční licenci, klikněte na tlačítko **Obnovit licenci**.

   Otevře se okno s webovou stránkou online obchodu Kaspersky, kde můžete zakoupit licenci.

Obnovení předplatného

Když aplikaci Kaspersky Endpoint Security používáte v rámci předplatného, aplikace se v určitých intervalech automaticky spojuje s aktivačním serverem, dokud neskončí platnost předplatného.

Když aplikaci Kaspersky Endpoint Security používáte v rámci neomezeného předplatného, aplikace na pozadí automaticky kontroluje, zda nejsou na aktivačním serveru k dispozici obnovené klíče. Pokud je na aktivačním serveru k dispozici klíč, aplikace jej přidá nahrazením předchozího klíče. Neomezené předplatné aplikace Kaspersky Endpoint Security se tímto způsobem obnovuje bez zásahu uživatele.

Pokud aplikaci používáte v rámci omezeného předplatného, v datu vypršení platnosti předplatného (nebo v datu vypršení platnosti lhůty pro obnovení předplatného) vás aplikace Kaspersky Endpoint Security na tuto skutečnost upozorní a již se nebude pokoušet o automatické obnovení předplatného. V tomto případě funguje aplikace Kaspersky Endpoint Security stejným způsobem jako při skončení platnosti komerční licence pro aplikaci: Aplikace funguje bez aktualizací a služba Kaspersky Security Network není k dispozici.

Předplatné můžete obnovit na webových stránkách poskytovatele služeb.

Stav předplatného můžete aktualizovat ručně pomocí okna **Správa licence**. Tento postup může být vyžadován, jestliže bylo obnoveno předplatné po poskytnuté lhůtě pro obnovení a aplikace neaktualizovala automaticky stav předplatného.

Navštívení webových stránek poskytovatele služeb prostřednictvím rozhraní aplikace:

1. V hlavním okně aplikace klikněte na tlačítko **Licence**.

2. V okně **Správa licence** klikněte na položku **Obraťte se na poskytovatele předplatného**.

Poskytování údajů na základě licenční smlouvy s koncovým uživatelem

Pokud je použit aktivační kód k aktivaci aplikace Kaspersky Endpoint Security, vyjadřujete souhlas s automatickým pravidelným zasíláním následujících informací pro účely ověření správného používání aplikace společnosti Kaspersky:

- typ, verze a lokalizace aplikace Kaspersky Endpoint Security;
- verze nainstalovaných aktualizací aplikace Kaspersky Endpoint Security;
- ID počítače a ID konkrétní instalace aplikace Kaspersky Endpoint Security v počítači;
- sériové číslo a identifikátor aktivního klíče;
- typ, verze a přenosová rychlost operačního systému a název virtuálního prostředí (pokud je aplikace Kaspersky Endpoint Security nainstalována ve virtuálním prostředí);
- ID součástí aplikace Kaspersky Endpoint Security, které jsou aktivní při přenosu informací.

Společnost Kaspersky může tyto informace také použít ke generování statistik distribuce a používání softwaru společnosti Kaspersky.

Použitím aktivačního kódu vyjadřujete souhlas s automatickým přenesením výše uvedených dat. Pokud s přenesením těchto informací společnosti Kaspersky nesouhlasíte, je třeba k aktivaci aplikace Kaspersky Endpoint Security použít soubor klíče.

Přijetím podmínek licenční smlouvy s koncovým uživatelem souhlasíte s automatickým přenesením následujících informací:

- V případě upgradu aplikace Kaspersky Endpoint Security:
  - verze aplikace Kaspersky Endpoint Security;
  - ID aplikace Kaspersky Endpoint Security;
  - aktivní klíč;
  - jedinečné ID spuštění úlohy upgradu;
  - jedinečné ID instalace aplikace Kaspersky Endpoint Security.
- V případě použití odkazů v rozhraní aplikace Kaspersky Endpoint Security:
  - verze aplikace Kaspersky Endpoint Security;
  - verze operačního systému;
  - datum aktivace aplikace Kaspersky Endpoint Security;
  - datum vypršení platnosti licence;

- datum vytvoření klíče;
- datum instalace aplikace Kaspersky Endpoint Security;
- ID aplikace Kaspersky Endpoint Security;
- ID zjištěného slabého místa v operačním systému;
- ID poslední nainstalované aktualizace aplikace Kaspersky Endpoint Security;
- hodnota hash zjištěného souboru s hrozbou a název této hrozby podle klasifikace společnosti Kaspersky;
- kategorie chyby aktivace aplikace Kaspersky Endpoint Security;
- kód chyby aktivace aplikace Kaspersky Endpoint Security;
- počet dní do vypršení platnosti klíče;
- počet dnů uplynulých od přidání klíče;
- počet dnů uplynulých od vypršení platnosti licence;
- počet počítačů s používanou aktivní licencí;
- aktivní klíč;
- licenční období aplikace Kaspersky Endpoint Security;
- aktuální stav licence;
- typ aktivní licence;
- typ aplikace;
- jedinečné ID spuštění úlohy upgradu;
- jedinečné ID instalace aplikace Kaspersky Endpoint Security v počítači;
- jazyk rozhraní aplikace Kaspersky Endpoint Security.

Přijaté informace jsou chráněny společností Kaspersky v souladu se zákonem a požadavky a platnými předpisy společnosti Kaspersky. Data jsou přenášena šifrovanými komunikačními kanály.

Přečtěte si licenční smlouvu s koncovým uživatelem a navštivte webové stránky společnosti Kaspersky, kde se dozvíte další informace o tom, jak přijímáme, zpracováváme, ukládáme a likvidujeme informace o využití aplikace poté, co potvrdíte souhlas s licenční smlouvou s koncovým uživatelem a vyjádříte souhlas s prohlášením služby Kaspersky Security Network. Soubory license.txt a ksn_<ID jazyka>.txt obsahují text licenční smlouvy s koncovým uživatelem a prohlášení služby Kaspersky Security Network a jsou obsaženy v distribučním balíčku aplikace.

Poskytování dat při používání služby Kaspersky Security Network

Sada dat, kterou aplikace Kaspersky Endpoint Security odesílá společnosti Kaspersky, závisí na typu licence a nastavení využití služby Kaspersky Security Network.

Používání KSN na základě licence na maximálně 4 počítačích

Přijetím prohlášení služby Kaspersky Security Network Statement souhlasíte s automatickým přenesením těchto informací:

- informace o aktualizacích konfigurace služby KSN: identifikátor aktivní konfigurace, identifikátor obdržené konfigurace, chybový kód aktualizace konfigurace;
- informace o souborech a adresách URL, které mají být kontrolovány: kontrolní součty kontrolovaného souboru (MD5, SHA2-256, SHA1) a vzory souboru (MD5), velikost vzoru, typ zjištěné hrozby a její název dle klasifikace nositele práv, identifikátor antivirových databází, adresa URL, pro kterou je požadována reputace, stejně jako adresa URL odkazujícího, identifikátor protokolu připojení a počet používaných portů;
- ID úlohy kontroly, která hrozbu detekovala;
- informace o používaných digitálních certifikátech potřebných k ověření jejich pravosti: kontrolní součty (SHA256) certifikátu použitého k podepsání kontrolovaného objektu a veřejný klíč certifikátu;
- identifikátor softwarové součásti provádějící kontrolu;
- ID antivirových databází a záznamů v těchto antivirových databázích;
- informace o aktivaci softwaru v počítači: podepsaná hlavička lístku od aktivační služby (identifikátor místního aktivačního střediska, kontrolní součet aktivačního kódu, kontrolní součet lístku, datum vytvoření lístku, jedinečný identifikátor lístku, verze lístku, stav licence, datum a čas zahájení a ukončení platnosti lístku, jedinečný identifikátor licence, verze licence), identifikátor certifikátu použitého k podepsání hlavičky lístku, kontrolní součet (MD5) souboru klíče;
- informace o softwaru držitele práv: plná verze, typ, verze protokolu použitého pro připojení ke službám společnosti Kaspersky.

Používání KSN na základě licence na maximálně 5 nebo více počítačích

Přijetím prohlášení služby Kaspersky Security Network Statement souhlasíte s automatickým přenesením těchto informací:

Pokud je zaškrtnuto políčko **Kaspersky Security Network** a není zaškrtnuto políčko **Rozšířený režim služby KSN**, aplikace odesílá následující informace:

- informace o aktualizacích konfigurace služby KSN: identifikátor aktivní konfigurace, identifikátor obdržené konfigurace, chybový kód aktualizace konfigurace;
- informace o souborech a adresách URL, které mají být kontrolovány: kontrolní součty kontrolovaného souboru (MD5, SHA2-256, SHA1) a vzory souboru (MD5), velikost vzoru, typ zjištěné hrozby a její název dle klasifikace nositele práv, identifikátor antivirových databází, adresa URL, pro kterou je požadována reputace, stejně jako adresa URL odkazujícího, identifikátor protokolu připojení a počet používaných portů;
- ID úlohy kontroly, která hrozbu detekovala;
- informace o používaných digitálních certifikátech potřebných k ověření jejich pravosti: kontrolní součty (SHA256) certifikátu použitého k podepsání kontrolovaného objektu a veřejný klíč certifikátu;
- identifikátor softwarové součásti provádějící kontrolu;
- ID antivirových databází a záznamů v těchto antivirových databázích;

- informace o aktivaci softwaru v počítači: podepsaná hlavička lístku od aktivační služby (identifikátor místního aktivačního střediska, kontrolní součet aktivačního kódu, kontrolní součet lístku, datum vytvoření lístku, jedinečný identifikátor lístku, verze lístku, stav licence, datum a čas zahájení a ukončení platnosti lístku, jedinečný identifikátor licence, verze licence), identifikátor certifikátu použitého k podepsání hlavičky lístku, kontrolní součet (MD5) souboru klíče;

- informace o softwaru držitele práv: plná verze, typ, verze protokolu použitého pro připojení ke službám společnosti Kaspersky.

Pokud je kromě políčka **Kaspersky Security Network** zaškrtnuto také políčko **Rozšířený režim služby KSN**, aplikace kromě výše uvedených informací odesílá také následující informace:

- informace o výsledcích kategorizace požadovaných webových zdrojů, které obsahují zpracovanou adresu URL a IP adresu hostujícího počítače, verzi komponenty softwaru, která kategorizaci provedla, metodu kategorizace a sadu kategorií definovaných pro webový zdroj;

- informace o softwaru instalovaném v počítači: názvy softwarových aplikací a jejich dodavatelů, klíčů registru a jejich hodnoty, informace o souborech nainstalovaných softwarových komponent (kontrolní součty (MD5, SHA2-256, SHA1), název, cesta k umístění souboru v počítači, velikost, verze a digitální podpis);

- informace o stavu antivirové ochrany počítače: verze a časové značky vydání použitých antivirových databází, ID úlohy a ID softwaru, který provádí kontrolu;

- informace o souborech stahovaných koncovým uživatelem: adresy URL a IP adresy stažených položek a stránky, ze kterých byly staženy, identifikátor protokolu stahování a číslo portu připojení, stav adres URL jako škodlivých nebo bezpečných, atributy, velikost a kontrolní součty souboru (MD5, SHA2-256, SHA1), informace o procesu, který soubor stáhl (kontrolní součty [MD5, SHA2-256, SHA1], datum a čas vytvoření/sestavení, stav automatického spuštění, atributy, názvy komprimačních nástrojů, informace o podpisech, příznak spustitelného souboru, identifikátor formátu a entropie), název souboru a cesta k jeho umístění v počítači, digitální podpis souboru a časová značka jeho vytvoření, adresa URL, kde došlo k nálezu, číslo skriptu na stránce, která se jeví jako podezřelá nebo škodlivá, informace o vygenerovaných požadavcích HTTP a odpovědích na ně;

- informace o spuštěných aplikacích a jejich modulech: data o spuštěných systémových procesech (ID nebo PID procesu, název procesu, informace o účtu, ze kterého byl proces spuštěn, aplikace a příkaz, které proces spustily, podpis důvěryhodného programu nebo procesu, úplná cesta k souborům procesu a jejich kontrolní součty (MD5, SHA2-256, SHA1) a spouštěcí příkazový řádek, úroveň integrity procesu, popis produktu, kterému proces náleží (název produktu a informace o vydavateli), stejně jako použité digitální certifikáty a informace potřebné k ověření jejich pravosti nebo informace o chybějícím digitálním podpisu souboru) a informace o modulech načtených do procesů (jejich názvy, velikosti, typy, data vytvoření, atributy, kontrolní součty (MD5, SHA2-256, SHA1), cesty k jejich umístění v počítači), informace o záhlaví souboru PE, názvy komprimačních nástrojů (pokud je soubor zkomprimován);

- informace o všech potenciálně škodlivých objektech a aktivitách: název zjištěného objektu a úplná cesta k objektu v počítači, kontrolní součty zpracovaných souborů (MD5, SHA2-256, SHA1), datum a čas zjištění, názvy a velikosti infikovaných souborů a cesty k nim, kód šablony cesty, příznak spustitelného souboru, ukazatel toho, zda je objekt kontejnerem, názvy komprimačního nástroje (pokud byl soubor zkomprimován), kód typu souboru, ID formátu souboru, seznam akcí provedených malwarem a rozhodnutí učiněné softwarem a uživatelem v reakci na ně, ID antivirových databází a záznamů v těchto antivirových databázích použitých k učinění rozhodnutí, indikátor potenciálně škodlivého objektu, název zjištěné hrozby podle klasifikace držitele práv, úroveň nebezpečí, stav zjištění a metoda zjištění, důvod zahrnutí do analyzovaného kontextu a pořadové číslo souboru v kontextu, kontrolní součty (MD5, SHA2-256, SHA1), název a atributy spustitelného souboru aplikace, prostřednictvím které byla přenesena infikovaná zpráva nebo odkaz, depersonalizované IP adresy (protokol IPv4 a IPv6) hostitele blokovaného objektu, entropie souboru, ukazatel automatického spuštění souboru, čas prvního zjištění souboru v systému, počet spuštění souboru od odeslání posledních statistik, informace o názvu, kontrolních součtech (MD5, SHA256, SHA1) a velikosti poštovního klienta, prostřednictvím kterého byl přijat škodlivý objekt, ID softwarové úlohy, která provedla kontrolu, ukazatel toho, zda byly zkontrolovány důvěryhodnost nebo podpis souboru, výsledek zpracování souboru, kontrolní součet (MD5) vzoru shromážděného pro objekt, velikost vzoru v bajtech a technické specifikace použitých technologií detekce;

- informace o kontrolovaných objektech: přiřazená důvěryhodná skupina, do které nebo ze které byl soubor umístěn nebo odebrán, důvod, proč byl soubor umístěn do dané kategorie, identifikátor kategorie, informace o zdroji kategorií a verze databáze kategorií, příznak důvěryhodného certifikátu souboru, název dodavatele souboru, verze souboru, název a verze softwarové aplikace, která obsahuje soubor;

- informace o zjištěných slabých místech: ID slabého místa v databázi slabých míst, třída nebezpečí slabého místa;

- informace o emulaci spustitelného souboru: velikost souboru a jeho kontrolní součty (MD5, SHA2-256, SHA1), verze komponenty emulace, hloubka emulace, pole vlastností logických bloků a funkcí v rámci logických bloků obdržených během emulace, data ze záhlaví PE spustitelného souboru;

- IP adresy počítače, který zaútočil (IPv4 a IPv6), číslo portu počítače, na který byl útok veden, identifikátor protokolu paketu IP obsahujícího útok, cíl útoku (název organizace, webová stránka), příznak reakce na útok, závažnost útoku, úroveň důvěryhodnosti;

- informace o útocích přidružených k falšovaným síťovým prostředkům, adresy DNS a IP adresy (IPv4 a IPv6) navštívených webových stránek;

- adresa DNS a IP adresa (IPv4 a IPv6) požadovaného webového prostředku, informace o souboru a webovém klientovi využívajícím webový prostředek, název, velikost a kontrolní součty (MD5, SHA2-256, SHA1) souboru, úplná cesta k souboru a kód šablony cesty, výsledek kontroly jeho digitálního podpisu a jeho stav podle služby KSN;

- informace o vrácení akcí malwaru: data o souboru, jehož aktivita byla vrácena zpět (název souboru, úplná cesta k souboru, jeho velikost a kontrolní součty (MD5, SHA2-256, SHA1)), data o úspěšných a neúspěšných akcích odstranění, přejmenování a kopírování souborů a obnovení hodnot v registru (názvy klíčů registru a jejich hodnoty) a informace o systémových souborech změněných malwarem, a to před vrácením změn a po něm;

- informace o výjimkách nastavených pro součást Adaptivní kontrola anomálií: ID a stav spuštěného pravidla, akce provedená softwarem při spuštění pravidla, typ uživatelského účtu, pod kterým proces nebo vlákno provádí podezřelou aktivitu, a informace o procesu, který provedl podezřelou aktivitu nebo jí byl vystaven (ID skriptu nebo název souboru procesu, úplná cesta k souboru procesu, kód šablony cesty, kontrolní součty (MD5, SHA2-256, SHA1) souboru procesu); informace o objektu, který prováděl podezřelé aktivity, a o objektu, který byl podezřelým aktivitám vystaven (název klíče registru nebo název souboru, úplná cesta k souboru, kód šablony cesty a kontrolní součty (MD5, SHA2-256, SHA1) souboru);

- informace o načtených softwarových modulech: název, velikost a kontrolní součty (MD5, SHA2-256, SHA1) souboru modulu, úplná cesta k němu a kód šablony pro cestu, nastavení digitálního podpisu souboru modulu, datum a čas vytvoření podpisu, název subjektu a organizace, které podepsaly soubor modulu, identifikátor procesu, ve kterém byl modul načten, název dodavatele modulu a číslo indexu modulu ve frontě načtení;

- informace o kvalitě interakce softwaru se službami KSN: datum zahájení a ukončení a doba, po kterou byly statistiky generovány, informace o kvalitě požadavků a připojení ke každé použité službě KSN (ID služby KSN, počet úspěšných požadavků, počet požadavků s odpovědí z mezipaměti, počet neúspěšných požadavků (problémy se sítí, vypnutí služby KSN nastavení softwaru, nesprávné směrování), časový rozsah úspěšných požadavků, časový rozsah zrušených požadavků, časový rozsah požadavků s překročeným časovým limitem, počet připojení ke službě KSN z mezipaměti, počet úspěšných připojení ke službě KSN, počet neúspěšných připojení ke službě KSN, počet úspěšných transakcí, počet neúspěšných transakcí, časový rozsah úspěšných připojení ke službě KSN, časový rozsah neúspěšných připojení ke službě KSN, časový rozsah úspěšných transakcí, časový rozptyl neúspěšných transakcí);

- pokud je rozpoznán potenciálně škodlivý objekt, jsou poskytnuty informace o datech v paměti daného procesu: prvky hierarchie objektů systému (ObjectManager), data v paměti UEFI BIOS, názvy klíčů registru a jejich hodnoty;

- informace o událostech v protokolech systému: časová značka události, název protokolu, ve kterém byla událost nalezena, typ a kategorie události, název zdroje události a popis události;

- informace o síťových připojeních: verze a kontrolní součty (MD5, SHA2-256, SHA1) souboru, ze kterého byl spuštěn proces, který otevřel port, cesta k souboru procesu a jeho digitální podpis, místní a vzdálená IP adresa, číslo místního a vzdáleného portu připojení, stav připojení, časová značka otevření portu;

- informace o datu instalace a aktivace softwaru v počítači: ID partnera, který licenci prodal, sériové číslo licence, podepsané záhlaví lístku z aktivační služby (ID regionálního aktivačního centra, kontrolní součet aktivačního kódu, kontrolní součet lístku, datum vytvoření lístku, jedinečné ID lístku, verze lístku, stav licence, datum a čas zahájení/ukončení lístku, jedinečné ID licence, verze licence), ID certifikátu použitého k podepsání záhlaví lístku, kontrolní součet (MD5) souboru klíče, jedinečné ID instalace softwaru v počítači, typ a ID aktualizované aplikace, ID úlohy aktualizace;

- informace o sadě všech instalovaných aktualizací a sada nejnověji instalovaných/odebraných aktualizací, typ události, která způsobila odeslání informací o aktualizaci, doba od poslední aktualizace instalace, informace o všech aktuálně instalovaných antivirových databázích;

- informace o provozu softwaru v počítači: data o využití procesoru, data o využití paměti (privátní bajty, nestránkovaný fond, stránkovaný fond), počet aktivních vláken v softwarovém procesu a nevyřízené hrozby a doba trvání provozu softwaru před chybou;

- počet výpisů softwaru a systému (BSOD) od instalace softwaru a jeho poslední aktualizace, identifikátor verze modulu softwaru, který selhal, paměťový zásobník procesu softwaru, informace o antivirových databázích v době selhání;

- údaje o výpisu systému (BSOD): příznak označující výskyt BSOD v počítači, název ovladače, který způsobil BSOD, adresa a paměťový zásobník ovladače, příznak označující dobu trvání relace OS před výskytem BSOD, paměťový zásobník ovladače, který selhal, typ uloženého výpisu paměti, příznak relace OS, která před výpisem BSOD trvala více než 10 minut, jedinečný identifikátor výpisu, časová značka BSOD;

- informace o chybách nebo problémech s výkonem, ke kterým došlo při používání softwarových komponent: ID stavu softwaru, typ, kód, příčina a čas výskytu chyby, ID komponenty, modul a proces produktu, u kterého k chybě došlo, ID kategorie úlohy nebo aktualizace, během které došlo k chybě, protokoly ovladačů použitých softwarem (chybový kód, název modulu, název zdrojového souboru a řádek, ve kterém došlo k chybě);

- informace o aktualizacích antivirových databází a komponent softwaru: název, datum a časový údaj indexových souborů stažených během poslední aktualizace a stahovaných během aktuální aktualizace;

- informace o neočekávaném ukončení operace softwaru: vytvoření časové značky výpisu, jeho typ, typ události, která způsobila neočekávané ukončení operace softwaru (neočekávané přerušení napájení, selhání aplikace třetí strany), datum a čas neočekávaného přerušení napájení;

- informace o kompatibilitě ovladačů softwaru s hardwarem a softwarem: informace o vlastnostech OS, které omezují fungování komponent softwaru (Secure Boot, KPTI, WHQL Enforce, BitLocker, rozlišování velikosti písma), typ nainstalovaného stahovacího softwaru (UEFI, BIOS), identifikátor Trusted Platform Module (TPM), specifikace verze TPM, informace o procesoru instalovaném v počítači, provozní režim a parametry integrity kódu a režimu Device Guard, provozní režim ovladačů a důvod použití stávajícího režimu, verze ovladačů softwaru, stav podpory virtualizace softwaru a hardwaru na počítači;

- informace o aplikacích třetích stran, které chybu způsobily: jejich název, verze a umístění, chybový kód a informace o chybě ze systémového protokolu aplikací, adresa chyby a paměťový zásobník aplikace třetí strany, příznak označující výskyt chyby v komponentě softwaru, doba, po kterou aplikace třetí strany fungovala, než došlo k chybě, kontrolní součty (MD5, SHA2-256, SHA1) obrazu procesu aplikace, ve kterém k chybě došlo, cesta k obrazu procesu aplikace a kód šablony cesty, informace ze systémového protokolu s popisem chyby přidružené k aplikaci, informace o režimu aplikace, ve které k chybě došlo (identifikátor výjimky, paměťová adresa selhání jako logická adresa v modulu aplikace, název a verze modulu, identifikátor selhání aplikace v modulu plugin nositele práv a paměťový zásobník selhání, doba trvání relace aplikace před selháním);

- verze komponenty aktualizátoru softwaru, počet selhání komponenty aktualizátoru při běhu úloh aktualizace během životnosti komponenty, ID typu úlohy aktualizace, počet neúspěšných pokusů komponenty aktualizátoru

o dokončení úloh aktualizace;

- informace o provozu komponent monitorování systému softwaru: plné verze komponent, datum a čas spuštění komponent, kód události, která přetekla frontu události, a počet takových událostí, celkový počet událostí přetečení fronty, informace o souboru procesu iniciátoru události (název souboru a jeho cesta v počítači, kód šablony cesty k souboru, kontrolní součty [MD5, SHA2-256, SHA1] procesu přidruženého k souboru, verze souboru), identifikátor zachycení události, ke kterému došlo, plná verze filtru zachycení, identifikátor typu zachycené události, velikost fronty událostí a počet událostí mezi první událostí ve frontě a aktuální událostí, počet zpožděných událostí ve frontě, informace o souboru procesu iniciátoru aktuální události (název souboru a jeho cesta v počítači, kód šablony cesty k souboru, kontrolní součty [MD5, SHA2-256, SHA1] procesu přidruženého k souboru), doba trvání zpracování události, maximální doba trvání zpracování události, pravděpodobnost odeslání statistik, informace o událostech operačního systému, u kterých byl překročen časový limit zpracování (datum a čas události, počet opakovaných inicializací antivirové databáze, datum a čas poslední opakované inicializace antivirových databází po jejich aktualizaci, doba zpoždění zpracování událostí u každé komponenty monitorování systému, počet událostí ve frontě, počet zpracovaných událostí, počet zpožděných událostí stávajícího typu, celková doba zpoždění u událostí stávajícího typu, celková doba zpoždění u všech událostí);

- informace z nástroje Windows pro sledování událostí (Event Tracing for Windows, ETW) v případě problémů s výkonem softwaru, dodavatelé událostí SysConfig/SysConfigEx/WinSATAssessment od společnosti Microsoft: informace o počítači (model, výrobce, formát skříně, verze), informace o výkonnostních metrikách systému Windows (hodnocení WinSAT, index výkonnosti systému Windows), název domény, informace o fyzických a logických procesorech (počet fyzických a logických procesorů, výrobce, model, číslo verze, počet jader, hodinový takt, CPUID, vlastnosti mezipaměti, vlastnosti logického procesoru, indikátory podporovaných režimů a pokynů), informace o modulech RAM (typ, formát, výrobce, model, kapacita, granulární povaha přidělení paměti), informace o síťových rozhraních (adresy IP a MAC, název, popis, konfigurace síťových rozhraní, rozdělení počtu a velikosti síťových balíčků podle typu, analýza síťové výměny, analýza počtu chyb sítě podle typu), konfigurace řadiče IDE, IP adresy serverů DNS, informace o grafické kartě (model, popis, výrobce, kompatibilita, kapacita grafické paměti, oprávnění obrazovky, počet bitů na pixel, verze systému BIOS), informace o zařízeních plug-and-play (název, popis, identifikátor zařízení [PnP, ACPI], informace o discích a úložných zařízeních (počet disků nebo jednotek flash, výrobce, model, kapacita disku, počet cylindrů, počet stop na cylindr, počet oddílů na sektor, kapacita sektoru, vlastnosti mezipaměti, sekvenční číslo, počet oddílů, konfigurace řadiče SCSI), informace o logických discích (sekvenční číslo, kapacita oddílu, kapacita svazku, písmeno svazku, typ oddílu, typ souborového systému, počet clusterů, velikost clusteru, počet sektorů na cluster, počet prázdných a využitých clusterů, písmeno spouštěcího svazku, offsetová adresa oddílu vzhledem k začátku disku), informace o základní desce BIOS (výrobce, datum výroby, verze), informace o základní desce (výrobce, model, typ), informace o fyzické paměti (sdílená a volná kapacita), informace o službách operačního systému (název, popis, stav, štítek, informace o procesech [název a PID]), parametry spotřeby energie počítače, konfigurace řadiče přerušení, cesta do systémových složek Windows (Windows a System32), informace o OS (verze, sestavení, datum vydání, název, typ, datum instalace), velikost stránkovacího souboru, informace o monitorech (počet, výrobce, oprávnění obrazovky, možnosti rozlišení, typ), informace o ovladači grafické karty (výrobce, datum výroby, verze);

- informace z nástroje ETW, dodavatelé událostí EventTrace/EventMetadata od společnosti Microsoft: informace o pořadí systémových událostí (typ, čas, datum, časové pásmo), metadata souboru s výsledky trasování (název, struktura, parametry trasování, analýza počtu operací trasování podle typu), informace o OS (název, typ, verze, sestavení, datum vydání, čas spuštění);

- informace z nástroje ETW, dodavatelé událostí Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power od společnosti Microsoft: informace o zahájených a dokončených procesech (název, PID, parametry spuštění, příkazový řádek, kód návratu, parametry správy napájení, čas zahájení a dokončení, typ přístupového tokenu, SID, SessionID, počet instalovaných deskriptorů), informace o změnách priorit vlákna (TID, priorita, čas), informace o operacích disku v procesu (typ, čas, kapacita, počet), historie změn struktury a kapacity procesů použitelné paměti;

- informace z nástroje ETW, dodavatelé událostí StackWalk / Perfinfo od společnosti Microsoft: informace o měřičích výkonu (výkon jednotlivých částí kódu, sekvence funkčních volání, PID, TID, adresy a atributy mechanismů ISR a DPC);

- informace z nástroje ETW, dodavatelé událostí KernelTraceControl-ImageID od společnosti Microsoft: informace o spustitelných souborech a dynamických knihovnách (název, velikost bitové kopie, úplná cesta), informace o souborech PDB (název, identifikátor), data prostředků VERSIONINFO pro spustitelné soubory (název, popis, tvůrce, umístění, verze a identifikátor aplikace, verze a identifikátor souboru);

- informace z nástroje ETW, dodavatelé událostí FileIo / DiskIo / Image / Windows Kernel Disk od společnosti Microsoft: informace o operacích souboru a disku (typ, kapacita, čas spuštění, čas dokončení, trvání, stav dokončení, PID, TID, adresy volání funkce ovladače, I/O Request Packet (IRP), atributy objektu souboru Windows), informace o souborech zapojených do operací souboru a disku (název, verze, velikost, úplná cesta, atributy, offset, kontrolní součet bitové kopie, možnosti otevření a přístupu);

- informace z nástroje ETW, dodavatelé událostí PageFault od společnosti Microsoft: informace o chybách přístupu ke stránce paměti (adresa, čas, kapacita, PID, TID, atributy objektu souboru systému Windows, parametry přidělení paměti);

- informace z nástroje ETW, dodavatelé událostí Thread od společnosti Microsoft: informace o vytváření/dokončení vláken, informace o spuštěných vláknech (PID, TID, velikost zásobníku, priority a přidělení zdrojů CPU, zdroje I/O, paměťové stránky mezi vlákny, adresa zásobníku, adresa funkce inicializace, adresa prvku Thread Environment Block (TEB), servisní štítek systému Windows);

- informace z nástroje ETW, dodavatelé událostí Microsoft Windows Kernel Memory od společnosti Microsoft: informace o operacích správy paměti (stav dokončení, čas, množství, PID), struktura přidělení paměti (typ, kapacita, SessionID, PID);

- informace o provozu softwaru v případě problémů s výkonem: identifikátor instalace softwaru, typ a hodnota poklesu výkonu, informace o sekvenci událostí v softwaru (čas, časové pásmo, typ, stav dokončení, identifikátor komponenty softwaru, identifikátor operačního scénáře softwaru, TID, PID, adresy volání funkce), informace o síťových připojeních ke kontrole (adresa URL, směr připojení, velikost síťového balíčku), informace o souborech PDB (název, identifikátor, velikost bitové kopie spustitelného souboru), informace o souborech ke kontrole (název, úplná cesta, kontrolní součet), parametry monitorování výkonu softwaru;

- informace o posledním úspěšném restartování OS: počet neúspěšných restartování od instalace OS, údaje týkající se výpisu systému (kód a parametry chyby, název, verze a kontrolní součet [CRC32] modulu, který způsobil chybu v operaci OS, adresa chyby jako logická adresa modulu, kontrolní součty [MD5, SHA2-256, SHA1] výpisu systému);

- informace k ověření pravosti digitálních certifikátů používaných k podepsání souborů: otisk prstu na certifikátu, algoritmus kontrolního součtu, veřejný klíč a sériové číslo certifikátu, název vystavitele certifikátu, výsledek ověření certifikátu a identifikátor databáze certifikátu;

- informace o procesu, který útočí na sebeobranu softwaru: název a velikost souboru procesu, jeho kontrolní součty (MD5, SHA2-256, SHA1), úplná cesta k souboru procesu a kód šablony cesty k souboru, časové značky vytvoření/sestavení, příznak spustitelného souboru, atributy souboru procesu, informace o certifikátu použitém k podepsání souboru procesu, kód účtu použitého ke spuštění procesu, ID operací provedených za účelem přístupu k procesu, typ prostředku, pomocí kterého je operace provedena (proces, soubor, objekt registru, funkce vyhledávání FindWindow), název prostředku, pomocí kterého je operace provedena, příznak označující úspěch operace, stav souboru procesu a jeho podpis podle služby KSN;

- informace o softwaru držitele práv: plná verze, typ, lokalizace a provozní stav použitého softwaru, verze nainstalovaných softwarových komponent a jejich provozní stav, informace o nainstalovaných aktualizacích softwaru, hodnota filtru TARGET, verze použitého protokolu sloužícího k připojení ke službám držitele práv;

- informace o hardwaru instalovaném v počítači: typ, název, název modelu, verze firmwaru, parametry vestavěných a připojených zařízení, jedinečný identifikátor počítače s instalovaným softwarem;

- informace o verzích operačního systému a instalovaných aktualizacích, velikost slova, verze a parametry režimu spuštění OS, verze a kontrolní součty (MD5, SHA2-256, SHA1) souboru jádra OS a datum a čas spuštění OS;

- spustitelné a nespustitelné soubory, ať už zcela nebo částečně;
- části paměti RAM počítače;
- sektory, jež jsou součástí procesu spuštění OS;
- datové pakety v síťovém provozu;
- webové stránky obsahující podezřelé a škodlivé objekty;
- popis tříd a instancí tříd úložiště WMI;
- zprávy o aktivitě aplikací:
    - název, velikost a verze odesílaného souboru, jeho popis a kontrolní součty (MD5, SHA2-256, SHA1), identifikátor formátu souboru, jméno dodavatele souboru, název produktu, ke kterému soubor patří, úplná cesta k souboru v počítači, kód šablony cesty, časové značky vytvoření a úpravy souboru;
    - počáteční a koncové datum a čas období platnosti certifikátu (pokud má soubor digitální podpis), datum a čas podpisu, jméno vydavatele certifikátu, informace o držiteli certifikátu, otisk prstu, veřejný klíč certifikátu a příslušné algoritmy a sériové číslo certifikátu;
    - název účtu, ze kterého je proces spuštěn;
    - kontrolní součty (MD5, SHA2-256, SHA1) názvu počítače, ve kterém je spuštěn proces;
    - názvy oken procesu;
    - Identifikátor antivirových databází, název zjištěné hrozby podle klasifikace držitelů práv;
    - údaje o nainstalované licenci, jejím identifikátoru, typu a datu konce platnosti;
    - místní čas počítače v okamžiku poskytnutí informace;
    - názvy a cesty k souborům, k nimž proces přistoupil;
    - názvy klíčů registru a jejich hodnoty, ke kterým proces přistoupil;
    - URL a IP adresy, ke kterým proces přistoupil;
    - URL a IP adresy, ze kterých byl spuštěný soubor stažen.

Soulad s právními předpisy Evropské unie (GDPR)

Aplikace Kaspersky Endpoint Security může přenášet společnosti Kaspersky data za následujících scénářů:

- Používání služby Kaspersky Security Network
- Aktivace aplikace pomocí aktivačního kódu
- Aktualizace modulů a antivirových databází aplikace
- Sledování odkazů v rozhraní aplikace

- Zápis souborů výpisu

Bez ohledu na klasifikaci dat a území, ze kterého jsou data přijímána, společnost Kaspersky dodržuje vysoké standardy pro zabezpečení dat a používá různá zákonná, organizační a technická opatření k ochraně dat uživatelů, k zajištění bezpečnosti a důvěrnosti dat a také k zajištění plnění práv uživatelů zaručených platnou legislativou. Text zásad ochrany osobních údajů je obsažen v sadě pro distribuci aplikací a je k dispozici na webu společnosti Kaspersky.

Před použitím aplikace Kaspersky Endpoint Security si pečlivě přečtěte popis přenášených dat v licenční smlouvě s koncovým uživatelem a v prohlášení ke službě Kaspersky Security Network. Pokud lze konkrétní data přenášená z aplikace Kaspersky Endpoint Security podle kteréhokoli z popsaných scénářů klasifikovat jako osobní údaje podle místních zákonů nebo norem, musíte zajistit, aby byla tato data zpracovávána zákonně, a získat se shromažďováním a přenosem takovýchto dat souhlas koncových uživatelů.

Přečtěte si licenční smlouvu s koncovým uživatelem a navštivte webové stránky společnosti Kaspersky, kde se dozvíte další informace o tom, jak přijímáme, zpracováváme, ukládáme a likvidujeme informace o využití aplikace poté, co potvrdíte souhlas s licenční smlouvou s koncovým uživatelem a vyjádříte souhlas s prohlášením služby Kaspersky Security Network. Soubory license.txt a ksn_<ID jazyka>.txt obsahují text licenční smlouvy s koncovým uživatelem a prohlášení služby Kaspersky Security Network a jsou obsaženy v distribučním balíčku aplikace.

Pokud společnosti Kaspersky data nechcete přenášet, můžete zakázat jejich poskytování.

Používání služby Kaspersky Security Network

Používáním aplikace Kaspersky Security Network souhlasíte s automatickým poskytováním údajů uvedených v prohlášení ke službě Kaspersky Security Network. Pokud nesouhlasíte s poskytováním těchto údajů společnosti Kaspersky, použijte privátní KSN nebo deaktivujte používání KSN. Více informací o privátní KSN naleznete v *dokumentaci k aplikaci Kaspersky Private Security Network*.

Aktivace aplikace pomocí aktivačního kódu

Použitím aktivačního kódu souhlasíte s automatickým poskytováním dat uvedených v licenční smlouvě s koncovým uživatelem. Pokud s přenášením těchto dat společnosti Kaspersky nesouhlasíte, je třeba k aktivaci aplikace Kaspersky Endpoint Security použít soubor klíče.

Aktualizace modulů a antivirových databází aplikace

Používáním serverů společnosti Kaspersky souhlasíte s automatickým poskytováním dat uvedených v licenční smlouvě s koncovým uživatelem. Společnost Kaspersky vyžaduje tyto informace k ověření, zda je aplikace Kaspersky Endpoint Security legitimně používána. Pokud s poskytováním těchto informací společnosti Kaspersky nesouhlasíte, použijte pro aktualizace databází služby Kaspersky Security Center nebo Kaspersky Update Utility.

Sledování odkazů v rozhraní aplikace

Používáním odkazů v rozhraní aplikace souhlasíte s automatickým poskytováním dat uvedených v licenční smlouvě s koncovým uživatelem. Přesný seznam dat přenášených v každém konkrétním odkazu závisí na tom, kde se odkaz nachází v rozhraní aplikace a jaký problém má za cíl vyřešit. Pokud s poskytováním těchto údajů společnosti Kaspersky nesouhlasíte, použijte zjednodušené rozhraní aplikace nebo skryjte rozhraní aplikace.

Zápis souborů výpisu

Pokud jste zápis výpisu paměti, aplikace Kaspersky Endpoint Security vytvoří soubor výpisu, který bude obsahovat všechna data paměti z procesů aplikace v okamžiku, kdy byl tento výpis vytvořen.

Začínáme

Po instalaci aplikace Kaspersky Endpoint Security můžete aplikaci spravovat pomocí následujících rozhraní:

- Místní rozhraní aplikace.
- Konzola pro správu aplikace Kaspersky Security Center.
- Webová konzola aplikace Kaspersky Security Center 12.
- Cloudová konzola aplikace Kaspersky Security Center.

Konzola pro správu aplikace Kaspersky Security Center.

Aplikace Kaspersky Security Center vám umožní aplikaci Kaspersky Endpoint Security vzdáleně instalovat a odinstalovat, spustit a zastavit, konfigurovat její nastavení, změnit sadu dostupných součástí aplikace, přidat klíče a spustit a zastavit úlohy aktualizace a kontroly.

Aplikaci lze spravovat prostřednictvím aplikace Kaspersky Security Center pomocí modulu plug-in administrace produktu Kaspersky Endpoint Security.

Podrobnější informace o správě aplikace pomocí rozhraní Kaspersky Security Center *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Webová konzola aplikace Kaspersky Security Center 12 a cloudová konzola aplikace Kaspersky Security Center.

Webová konzola aplikace Kaspersky Security Center 12 (dále označována také jako „*webová konzola*“) je webová aplikace určená k centrálnímu provádění hlavních úloh za účelem správy a udržování systému zabezpečení sítě organizace. Webová konzole je součást aplikace Kaspersky Security Center, která poskytuje uživatelské rozhraní. Podrobné informace webové konzole aplikace Kaspersky Security Center 12 *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Cloudová konzola Kaspersky Security Center (dále také „ *cloudová konzola* “) je cloudové řešení pro ochranu a správu sítě organizace. Podrobné informace o cloudové konzole aplikace Kaspersky Security Center *najdete v nápovědě ke cloudové konzole aplikace Kaspersky Security Center*.

Webová konzola a cloudová konzola vám umožní provádět následující akce:

- sledovat stav systému zabezpečení vaší organizace,
- instalovat aplikace společnosti Kaspersky do zařízení v síti,
- spravovat nainstalované aplikace,
- zobrazit zprávy o stavu systému zabezpečení.

Správa aplikace Kaspersky Endpoint Security prostřednictvím webové konzoly, cloudové konzoly a konzoly pro správu aplikace Kaspersky Security Center poskytuje různé možnosti správy. Pro různé konzoly se také liší dostupné součásti a úlohy.

O modulu plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows

Modul plug-in administrace produktu Kaspersky Endpoint Security pro systém Windows umožňuje interakci mezi aplikací Kaspersky Endpoint Security a aplikací Kaspersky Security Center. Modul plug-in pro správu umožňuje spravovat aplikaci Kaspersky Endpoint Security pomocí následujících nástrojů: zásady, úlohy a místní nastavení aplikace. Interakce s webovou konzolou aplikace Kaspersky Security Center 12 je poskytována prostřednictvím webového pluginu.

Verze modulu plug-in administrace se liší od verze aplikace Kaspersky Endpoint Security nainstalované v klientském počítači. Pokud má nainstalovaná verze modulu plug-in administrace méně funkcí než nainstalovaná verze aplikace Kaspersky Endpoint Security, nastavení chybějících funkcí nebudou modulem řízeny. Toto nastavení může uživatel měnit v místním rozhraní aplikace Kaspersky Endpoint Security.

Webový modul plug-in není ve výchozím nastavení instalován ve Kaspersky Security Center 12 Web Console. Na rozdíl od modulu plug-in administrace pro konzoli pro správu aplikace Kaspersky Security Center, která se instaluje do pracovní stanice správce, je nutné webový modul plug-in nainstalovat do počítače, ve kterém je nainstalována Kaspersky Security Center 12 Web Console. Funkce webového modulu plug-in je k dispozici pro všechny správce, kteří mají přístup k webové konzoli v prohlížeči. V rozhraní webové konzole můžete zobrazit seznam nainstalovaných webových modulů plug-in: **Console settings** → **Plug-ins**. Podrobnější informace o kompatibilitě verzí webových modulů plug-in a webové konzole najdete v *nápovědě k aplikaci Kaspersky Security Center*.

Instalace webového modulu plug-in

Webový modul plug-in lze nainstalovat následujícím způsobem:

- Nainstalujte webový modul plug-in pomocí Průvodce počáteční konfigurací Kaspersky Security Center 12 Web Console.

  Webová konzole vás automaticky vyzve, abyste spustili Průvodce počáteční konfigurací, během prvního připojení webové konzole k serveru pro správu. Průvodce počáteční konfigurací můžete také spustit v rozhraní webové konzole (**Device discovery and deployment** → **Deployment and assignment** → **Initial Configuration Wizard**). Průvodce počáteční konfigurací může také zkontrolovat, zda jsou nainstalované webové moduly plug-in aktuální, a může stáhnout potřebné aktualizace. Podrobnější informace o Průvodci počáteční konfigurací pro Kaspersky Security Center 12 Web Console najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

- Nainstalujte webový modul plug-in ze seznamu dostupných distribučních balíčků ve webové konzoli.

  Chcete-li nainstalovat webový modul plug-in, vyberte distribuční balíček webového modulu plug-in aplikace Kaspersky Endpoint Security v rozhraní webové konzole: **Console settings** → **Plug-ins**. Seznam dostupných distribučních balíčků je aktualizován automaticky po vydání nových verzí aplikací společnosti Kaspersky.

- Stáhněte distribuční balíček do webové konzole z externího zdroje.

  Chcete-li nainstalovat webový modul plug-in, přidejte archiv ZIP distribučního balíčku pro webový modul plug-in aplikace Kaspersky Endpoint Security do rozhraní webové konzole: **Console settings** → **Plug-ins**. Distribuční balíček webového modulu plug-in lze stáhnout například na webových stránkách společnosti Kaspersky.

Aktualizace modulu plug-in pro správu

Chcete-li aktualizovat modul plug-in administrace produktu Kaspersky Endpoint Security pro systém Windows, stáhněte si nejnovější verzi modulu (součástí distribuční sady) a spusťte průvodce instalací modulu.

Pokud je zpřístupněna nová verze webového modulu plug-in, webová konzole zobrazí oznámení *Updates are available for utilized plug-ins*. Z tohoto oznámení webové konzole můžete pokračovat k aktualizaci verze webového modulu plug-in. Můžete také ručně zjistit nové aktualizace webového modulu plug-in v rozhraní webové konzole (**Console settings** → **Plug-ins**). Během aktualizace bude automaticky odebrána předchozí verze webového modulu plug-in.

Po aktualizaci webového modulu plug-in jsou uloženy již existující položky (například zásady nebo úlohy). Nová nastavení položek, které zavádějí nové funkce aplikace Kaspersky Endpoint Security, se zobrazí v existujících položkách a budou mít výchozí nastavení.

Webový modul plug-in lze aktualizovat následujícím způsobem:

- Aktualizujte webový modul plug-in v seznamu webových modulů plug-in v online režimu.

  Chcete-li aktualizovat webový modul plug-in, je nutné vybrat distribuční balíček webového modulu plug-in aplikace Kaspersky Endpoint Security v rozhraní webové konzole (**Console settings** → **Plug-ins**). Webová konzole zjistí dostupné aktualizace na serverech společnosti Kaspersky a stáhne příslušné aktualizace.

- Aktualizujte webový modul plug-in ze souboru.

  Chcete-li aktualizovat webový modul plug-in, je nutné vybrat archiv ZIP distribučního balíčku pro webový modul plug-in aplikace Kaspersky Endpoint Security v rozhraní webové konzole: **Console settings** → **Plug-ins**. Distribuční balíček webového modulu plug-in lze stáhnout například na webových stránkách společnosti Kaspersky. Webový modul plug-in aplikace Kaspersky Endpoint Security můžete aktualizovat pouze na nejnovější verzi. Webový modul plug-in nelze aktualizovat na starší verzi.

V případě otevření jakékoli položky (například zásady nebo úlohy) zkontroluje webový modul plug-in informace o její kompatibilitě. Pokud je verze webového modulu plug-in stejná nebo vyšší než verze uvedená v informacích o kompatibilitě, můžete upravovat nastavení této položky. Pokud není, nelze webový modul plug-in používat ke změně nastavení vybrané položky. Doporučujeme vám aktualizovat webový modul plug-in.

Zvláštní požadavky na práci s různými verzemi modulů plug-in administrace

Aplikaci Kaspersky Endpoint Security můžete spravovat prostřednictvím aplikace Kaspersky Security Center, pouze pokud máte modul plug-in administrace verze stejné nebo vyšší, než je verze uvedená v informacích o kompatibilitě aplikace Kaspersky Endpoint Security s modulem plug-in administrace. Minimální požadovanou verzi modulu plug-in administrace můžete zobrazit v souboru installer.ini, který je součástí distribuční sady.

V případě otevření jakékoli položky (například zásady nebo úlohy) zkontroluje modul plug-in administrace informace o její kompatibilitě. Pokud je verze modulu plug-in administrace stejná nebo vyšší než verze uvedená v informacích o kompatibilitě, můžete upravovat nastavení této položky. Pokud není, nelze modul plug-in administrace používat k upravování nastavení dané položky. Doporučujeme vám upgradovat modul plug-in administrace.

Upgrade modulu plug-in administrace aplikace Kaspersky Endpoint Security 10 pro systém Windows

Pokud je v konzoli pro správu nainstalován modul plug-in administrace produktu Kaspersky Endpoint Security 10 pro systém Windows, při instalaci modulu plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows zvažte následující skutečnosti:

- Modul plug-in administrace produktu Kaspersky Endpoint Security 10 pro systém Windows nebude odebrán a bude jej možné i nadále používat. Proto budete mít přístup ke dvěma modulům plug-in administrace pro práci s aplikací verze 10 a 11.
- Modul plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows nepodporuje správu aplikace Kaspersky Endpoint Security 10 pro systém Windows v počítačích uživatelů.
- Modul plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows nepodporuje položky (například zásady nebo úlohy), které byly vytvořeny pomocí modulu plug-in administrace produktu Kaspersky Endpoint Security 10 pro systém Windows.

  K převodu zásad a úloh z verze 10 na verzi 11 můžete použít průvodce hromadným převodem zásad a úkolů. Další informace o převodu zásad a úloh najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

Upgrade modulu plug-in administrace aplikace Kaspersky Endpoint Security 10 pro systém Windows

Pokud je v konzoli pro správu nainstalován modul plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows, při instalaci nové verze modulu plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows zvažte následující skutečnosti:

- Předchozí verze modulu plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows bude odebrána.
- Nová verze modulu plug-in administrace produktu Kaspersky Endpoint Security 11 pro systém Windows podporuje správu předchozí verze aplikace Kaspersky Endpoint Security 11 pro systém Windows v počítačích uživatelů.
- Pomocí nové verze modulu plug-in administrace můžete změnit nastavení v zásadách, úlohách a další položky vytvořené předchozí verzí modulu plug-in administrace.
- Při prvním uložení zásad, profilu zásad nebo úlohy přiřadí nová verze modulu plug-in administrace novým nastavením výchozí hodnoty.

  Po upgradu modulu plug-in administrace se doporučuje zkontrolovat a uložit hodnoty nových nastavení v zásadách a profilech zásad. Pokud to neuděláte, nové skupiny nastavení aplikace Kaspersky Endpoint Security v počítači uživatele budou mít výchozí hodnoty a mohou být upraveny (atribut ). Doporučuje se zkontrolovat nastavení, počínaje zásadami a profily zásad v nejvyšší úrovni hierarchie. Také se doporučuje použít uživatelský účet, který má přístupová práva ke všem funkčním oblastem aplikace Kaspersky Security Center.

  Chcete-li získat informace o nových možnostech aplikace, přečtěte si poznámky k verzi nebo nápovědu k aplikaci.

- Pokud byl v nové verzi modulu plug-in administrace přidán do skupiny nastavení nový parametr, dříve definovaný stav atributu  /  pro tuto skupinu nastavení se nezmění.
- Při upgradu modulu plug-in administrace na verzi 11.2.0 je nutné zásadu otevřít, aby mohla být automaticky převedena. Při tom vás Kaspersky Endpoint Security vyzve k potvrzení účasti ve službě KSN. Pokud jste již v počítačích své organizace upgradovali aplikaci na verzi 11.20, bude účast v KSN deaktivována, dokud nepřijmete podmínky účasti v KSN.

Zvláštní úvahy při používání šifrovaných protokolů pro interakci s externími službami

Aplikace Kaspersky Endpoint Security a Kaspersky Security Center používají pro práci s externími službami společnosti Kaspersky šifrovaný komunikační kanál s vrstvou TLS (Transport Layer Security). Aplikace Kaspersky Endpoint Security používá externí služby pro následující funkce:

- Aktualizace databází a softwarových modulů aplikace
- Aktivace aplikace aktivačním kódem (aktivace 2.0)
- Používání služby Kaspersky Security Network

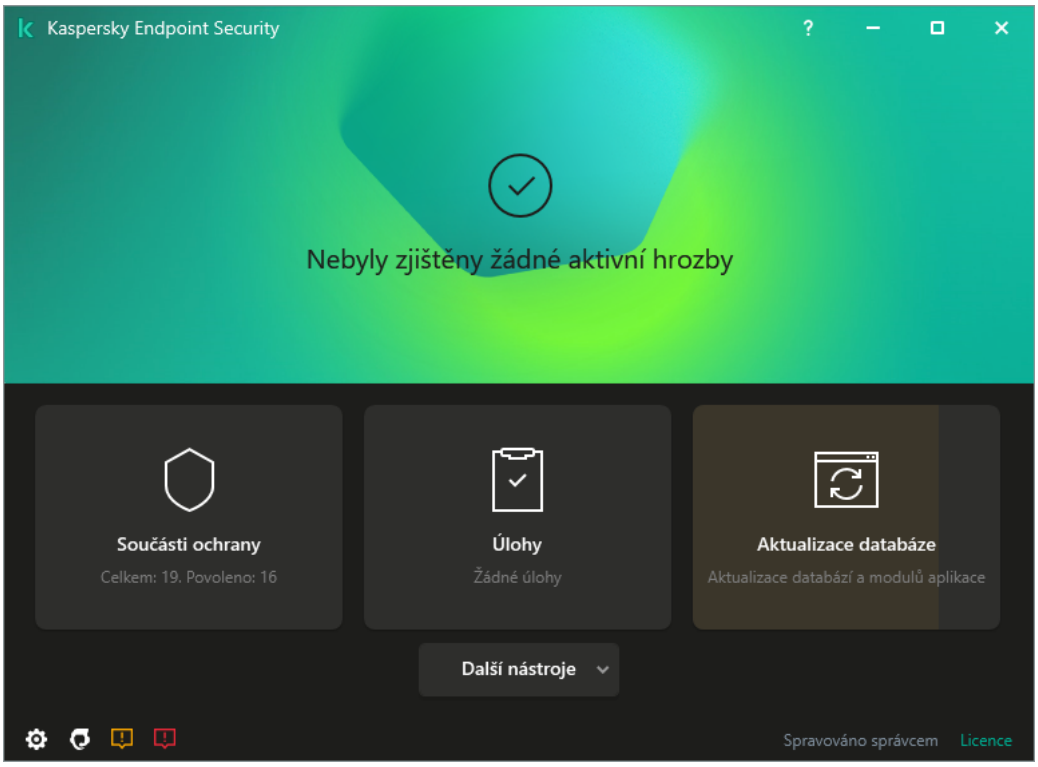
Použití protokolu TLS zajišťuje aplikaci poskytnutím následujících funkcí:

- Šifrování. Obsah zpráv je důvěrný a není sdělován uživatelům třetích stran.
- Integrita. Příjemce zprávy si je jistý, že obsah zprávy nebyl od odeslání odesílatelem změněn.
- Ověřování. Příjemce si je jistý, že komunikace je navázána pouze s důvěryhodným serverem Kaspersky.

Kaspersky Endpoint Security používá k ověření serveru certifikáty veřejného klíče. Pro práci s certifikáty je vyžadována infrastruktura veřejného klíče (PKI). Součástí PKI je certifikační autorita. Společnost Kaspersky používá vlastní certifikační autoritu, protože služby Kaspersky jsou vysoce technické a neveřejné. Díky tomu zůstanou v případě zrušení kořenových certifikátů Thawte, VeriGisn, GlobalTrust a dalších zůstane Kaspersky PKI funkční bez přerušení.

Prostředí s MITM (softwarové a hardwarové nástroje, které podporují analýzu protokolu HTTPS) považuje Kaspersky Endpoint Security za nebezpečná. Při práci se službami Kaspersky se mohou vyskytnout chyby. Mohou se například vyskytnout chyby týkající se použití certifikátů podepsaných svým držitelem. Tyto chyby mohou nastat, protože nástroj HTTPS Inspection z vašeho prostředí nerozpozná PKI společnosti Kaspersky. Chcete-li tyto problémy napravit, musíte nakonfigurovat výjimky pro interakci s externími službami.

Rozhraní aplikace



Hlavní okno aplikace

Součásti ochrany	Provozní stav nainstalovaných součástí. Můžete také pokračovat v konfiguraci kterékoli z nainstalovaných součástí kromě součástí šifrování.
Úlohy	Můžete spravovat úlohy kontroly aplikace Kaspersky Endpoint Security. Můžete spustit antivirovou kontrolu a kontrolu integrity aplikace. Správce může skrýt úlohy před uživatelem nebo omezit správu úloh.
Aktualizace databáze	Můžete spravovat úlohy aktualizace aplikace Kaspersky Endpoint Security. Můžete aktualizovat antivirové databáze a moduly aplikace a vrátit zpět poslední aktualizaci. Správce může skrýt úlohy před uživatelem nebo omezit správu úloh.
Další nástroje	Pokračování k dalším funkcím aplikace. • **Zprávy**. Zobrazení událostí, ke kterým došlo během provozu aplikace, jednotlivých součástí a úloh. • **Záloha**. Zobrazení seznamu uložených kopií infikovaných souborů, které aplikace odstranila. • **Technologie detekce hrozeb**. Zobrazení informací o technologiích detekce hrozeb a počtu hrozeb detekovaných těmito technologiemi. • **Kaspersky Security Network**. Stav připojení mezi aplikací Kaspersky Endpoint Security a Kaspersky Security Network a globální statistikou KSN. *Služba Kaspersky Security Network (KSN)* představuje infrastrukturu cloudových služeb, která poskytuje přístup k internetové znalostní bázi společnosti Kaspersky s informacemi o reputaci souborů, webových prostředcích a softwaru. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikace Kaspersky Endpoint Security na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků. Jestliže se účastníte služby Kaspersky Security Network, služby KSN poskytují aplikaci Kaspersky Endpoint Security informace o kategorii a pověsti naskenovaných souborů a také informace o pověsti kontrolovaných webových adres. • **System Watcher**. Zobrazení informací o provozu nainstalovaných aplikací. System Watcher sleduje události souborů, registru a systému související s aplikací. • **Sledování sítě**. Zobrazení informací o síťové aktivitě počítače v reálném čase.

	• **Sledování šifrování**. Sleduje proces šifrování nebo dešifrování disku v reálném čase. Nástroj Sledování šifrování je k dispozici, pokud je nainstalována součást Kaspersky Disk Encryption nebo součást BitLocker Drive Encryption.
⚙	Konfigurace nastavení aplikace. Správce může zakázat změny nastavení v aplikaci Kaspersky Security Center.
	Informace o aplikaci: aktuální verze aplikace Kaspersky Endpoint Security, datum vydání databáze, klíč a další informace. Můžete také přejít na informační zdroje aplikace Kaspersky, které poskytují užitečné informace, doporučení a odpovědi na časté dotazy o koupi, instalaci a používání aplikace.
/	Zprávy obsahující informace o dostupných aktualizacích a požadavcích na přístup k šifrovaným souborům a zařízením.
Licence	Správa licence k aplikaci. Můžete si zakoupit licenci, aktivovat aplikaci nebo obnovit předplatné. Můžete také zobrazit informace o aktuální licenci.

Ikona Aplikace v oznamovací oblasti hlavního panelu

Ihned po instalaci aplikace Kaspersky Endpoint Security se v oznamovací oblasti hlavního panelu systému Microsoft Windows zobrazí ikona aplikace.

Tato ikona slouží k následujícím účelům:

- Označuje činnost aplikace.
- Slouží jako zástupce kontextové nabídky a hlavního okna aplikace.

Pro zobrazení informací o provozu aplikace jsou k dispozici následující stavy ikon aplikace:

- Ikona značí, že všechny kriticky důležité součásti ochrany aplikace jsou povolené. Pokud má uživatel provést akci, například po aktualizaci aplikace restartovat počítač, aplikace Kaspersky Endpoint Security zobrazí upozornění .
- Ikona značí, že jsou deaktivovány nebo jsou nefunkční kriticky důležité součásti ochrany aplikace. Součásti ochrany mohou být nefunkční například v případě, že vypršela platnost licence nebo v důsledku chyby aplikace. Aplikace Kaspersky Endpoint Security zobrazí upozornění s popisem problému s ochranou počítače.

Kontextová nabídka ikony aplikace obsahuje tyto položky:

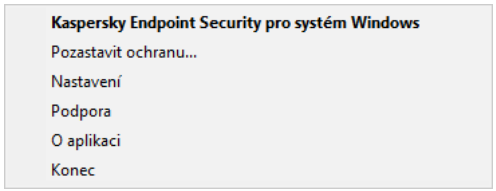
- **Kaspersky Endpoint Security pro systém Windows**. Otevře hlavní okno aplikace. V tomto okně můžete upravit fungování součástí a úloh aplikace a také zobrazit statistiky o zpracovaných souborech a zjištěných hrozbách.
- **Pozastavit ochranu / Obnovit ochranu**. Pozastaví činnost všech součástí ochrany a kontroly, které nejsou v zásadách označeny zámkem (). Před provedením této operace doporučujeme zakázat zásady aplikace Kaspersky Security Center.

  Před pozastavením činnosti součástí ochrany a kontroly si aplikace vyžádá heslo pro přístup k aplikaci Kaspersky Endpoint Security (heslo účtu nebo dočasné heslo). Poté můžete vybrat dobu pozastavení: na určitou dobu, do restartu nebo na žádost uživatele.

  Tato položka místní nabídky je k dispozici, pokud je aktivována ochrana heslem. Chcete-li obnovit činnost součástí ochrany a kontroly, vyberte v místní nabídce aplikace možnost **Obnovit ochranu**.

Pozastavení činnosti součástí ochrany a kontroly nemá vliv na výkon úloh aktualizace a kontroly. Aplikace také pokračuje v používání služby Kaspersky Security Network.

- **Zakázat zásadu** / **Povolit zásadu**. Zakáže v počítači zásady sady softwaru Kaspersky Security Center. Všechna nastavení aplikace Kaspersky Endpoint Security jsou k dispozici pro konfiguraci, včetně nastavení, která mají v zásadách uzavřený zámek (). Jsou-li zásady zakázány, aplikace navíc vyžaduje heslo pro přístup k aplikaci Kaspersky Endpoint Security (heslo účtu nebo dočasné heslo). Tato položka místní nabídky je k dispozici, pokud je aktivována ochrana heslem. Chcete-li povolit zásadu, vyberte v místní nabídce aplikace možnost **Povolit zásadu**.
- Nastavení. Otevřete okno nastavení aplikace.
- **Podpora**. Pomocí této položky můžete otevřít okno **Podpora**, které obsahuje informace potřebné ke kontaktování technické podpory společnosti Kaspersky.
- **O aplikaci**. Tato položka otevře okno s podrobnými informacemi o aplikaci.
- **Konec**. Tato položka ukončí aplikaci Kaspersky Endpoint Security. Kliknutím na tuto položku kontextové nabídky dojde k uvolnění aplikace z paměti RAM počítače.



Kontextová nabídka ikony Aplikace

Zjednodušené rozhraní aplikace

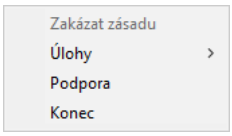
Pokud jsou na klientský počítač, ve kterém je nainstalována aplikace Kaspersky Endpoint Security, použity zásady aplikace Kaspersky Security Center nakonfigurované k zobrazení zjednodušeného rozhraní aplikace, není v tomto klientském počítači k dispozici hlavní okno aplikace. Když na ikonu aplikace Kaspersky Endpoint Security kliknete pravým tlačítkem myši, zobrazí se kontextová nabídka (viz obrázek níže) obsahující následující položky:

- **Zakázat zásadu** / **Povolit zásadu**. Zakáže v počítači zásady sady softwaru Kaspersky Security Center. Všechna nastavení aplikace Kaspersky Endpoint Security jsou k dispozici pro konfiguraci, včetně nastavení, která mají v zásadách uzavřený zámek (). Jsou-li zásady zakázány, aplikace navíc vyžaduje heslo pro přístup k aplikaci Kaspersky Endpoint Security (heslo účtu nebo dočasné heslo). Tato položka místní nabídky je k dispozici, pokud je aktivována ochrana heslem. Chcete-li povolit zásadu, vyberte v místní nabídce aplikace možnost **Povolit zásadu**.
- **Úlohy**. Rozevírací seznam obsahuje následující položky:
  - **Kontrola integrity**.
  - **Vrácení změn provedených poslední aktualizací**.
  - **Úplná kontrola**.
  - **Uživatelská kontrola**.
  - **Kontrola kritických oblastí**.

- **Aktualizace**.

- **Podpora**. Pomocí této položky můžete otevřít okno **Podpora**, které obsahuje informace potřebné ke kontaktování technické podpory společnosti Kaspersky.

- **Konec**. Tato položka ukončí aplikaci Kaspersky Endpoint Security. Kliknutím na tuto položku kontextové nabídky dojde k uvolnění aplikace z paměti RAM počítače.



Kontextová nabídka ikony aplikace při zobrazení zjednodušeného rozhraní

Konfigurace zobrazení rozhraní aplikace

Můžete nakonfigurovat režim zobrazení rozhraní aplikace pro uživatele. Uživatel může interagovat s aplikací následujícími způsoby:

- **Se zjednodušeným rozhraním**. V klientském počítači je hlavní okno aplikace nepřístupné a je k dispozici pouze ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel s aplikací Kaspersky Endpoint Security provádět omezený počet operací. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace.

- **S úplným rozhraním**. V klientském počítači je k dispozici hlavní okno aplikace Kaspersky Endpoint Security a ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel provádět operace s aplikací Kaspersky Endpoint Security. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace.

- **Žádné rozhraní**. V klientském počítači se nezobrazují žádné známky provozu aplikace Kaspersky Endpoint Security. Ikona v oznamovací oblasti systému Windows ani upozornění nejsou k dispozici.

Jak nakonfigurovat režim zobrazení rozhraní aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Obecná nastavení** → **Rozhraní**.
6. V části **Interakce s uživatelem** proveďte některou z následujících akcí:
   - Zaškrtněte políčko **Zobrazit rozhraní aplikace**, pokud chcete, aby se v klientském počítači zobrazily následující prvky rozhraní:
     - Složka obsahující název aplikace v nabídce **Start**
     - Ikona aplikace Kaspersky Endpoint Security v oznamovací oblasti hlavního panelu systému Microsoft Windows
     - Místní oznámení

     Pokud je toto políčko zaškrtnuté, uživatel může zobrazit a v závislosti na dostupných oprávněních změnit nastavení aplikace v rozhraní aplikace.
   - Zrušte zaškrtnutí políčka **Zobrazit rozhraní aplikace**, pokud chcete skrýt všechny známky přítomnosti aplikace Kaspersky Endpoint Security v klientském počítači.
7. V části **Interakce s uživatelem** zaškrtněte políčko **Zjednodušené rozhraní aplikace**, pokud chcete zobrazit zjednodušené rozhraní aplikace v klientském počítači s nainstalovanou aplikací Kaspersky Endpoint Security.

Jak nakonfigurovat místní nastavení aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete povolit podporu mobilního režimu.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Obecná nastavení** → **Rozhraní**.
5. V části **Interakce s uživatelem** nakonfigurujte způsob zobrazování rozhraní aplikace:
   - **Se zjednodušeným rozhraním**. V klientském počítači je hlavní okno aplikace nepřístupné a je k dispozici pouze ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel s aplikací Kaspersky Endpoint Security provádět omezený počet operací. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace.
   - **S úplným rozhraním**. V klientském počítači je k dispozici hlavní okno aplikace Kaspersky Endpoint Security a ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel provádět operace s aplikací Kaspersky Endpoint Security. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace.
   - **Žádné rozhraní**. V klientském počítači se nezobrazují žádné známky provozu aplikace Kaspersky Endpoint Security. Ikona v oznamovací oblasti systému Windows ani upozornění nejsou k dispozici.
6. Klikněte na tlačítko **OK**.

Začínáme

Pokud chcete po nasazení aplikace do klientských počítačů pracovat s aplikací Kaspersky Endpoint Security z webové konzoly aplikace Kaspersky Security Center, je nutné provést následující akce:

- Vytvořte a nakonfigurujte zásadu.

  Pomocí zásad můžete použít stejná nastavení aplikace Kaspersky Endpoint Security pro všechny klientské počítače v rámci skupiny správy. Průvodce počáteční konfigurací Kaspersky Security Center automaticky vytvoří zásadu pro aplikaci Kaspersky Endpoint Security.
- Vytvořte úlohy *Aktualizovat* a *Antivirová kontrola*.

  Úloha *Aktualizace* je třeba pro zachování aktuálního zabezpečení počítače. Když je provedena tato úloha, aplikace Kaspersky Endpoint Security aktualizuje antivirové databáze a moduly aplikace. Úloha *Aktualizace* je automaticky vytvořena průvodcem počáteční konfigurací aplikace Kaspersky Security Center. Chcete-li vytvořit úlohu *Aktualizace*, nainstalujte při spuštění průvodce webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

  Úloha *Antivirová kontrola* je třeba ke včasnému zjištění virů a dalšího malwaru. Musíte ručně vytvořit úlohu *Antivirová kontrola*.

Jak vytvořit úlohu antivirové kontroly v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnosti **Kaspersky Endpoint Security pro systém Windows (11.6.0)** → **Antivirová kontrola**.

Krok 2. Rozsah kontroly

Vytvoření seznamu objektů, které aplikace Kaspersky Endpoint Security kontroluje při provádění úlohy kontroly.

Krok 3. Akce aplikace Kaspersky Endpoint Security

Vyberte akci při zjištění hrozby:

- **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní.

- **Dezinfikovat; a pokud se dezinfekce nezdaří, tak informovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.

- **Informovat**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb.

- **Spustit pokročilou dezinfekci okamžitě**. Pokud je toto políčko zaškrtnuté, aplikace Kaspersky Endpoint Security používá ke zpracování aktivních hrozeb během kontroly technologii pokročilé dezinfekce.

  Technologie pokročilé dezinfekce je zaměřena na očištění operačního systému od škodlivých aplikací, které již spustily své procesy v paměti RAM a které brání aplikaci Kaspersky Endpoint Security v odstranění jinými způsoby. Výsledkem je neutralizace hrozby. Zatímco probíhá pokročilá dezinfekce, neměli byste spouštět nové procesy ani upravovat registr operačního systému. Technologie pokročilé dezinfekce je velmi náročná na prostředky operačního systému, což může způsobit zpomalení chodu jiných aplikací. Po provedení pokročilé dezinfekce aplikace Kaspersky Endpoint Security restartuje počítač, aniž by žádal uživatele o potvrzení.

Režim spuštění úlohy nakonfigurujete pomocí zaškrtávacího políčka **Spustit pouze v době, kdy je počítač neaktivní**. Tímto zaškrtávacím políčkem povolíte nebo zakážete funkci, která odloží úlohu *antivirové kontroly*, když jsou výpočetní prostředky omezené. Aplikace Kaspersky Endpoint Security pozastaví úlohu *antivirové kontroly*, když je vypnutý spořič obrazovky a počítač je odemčený.

Krok 4. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 5. Výběr účtu pro spuštění úlohy

Vyberte účet pro spuštění úlohy *antivirové kontroly*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu. Pokud rozsah kontroly zahrnuje síťové jednotky nebo jiné objekty s omezeným přístupem, vyberte uživatelský účet s dostatečnými přístupovými právy.

Krok 6. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně nebo po stažení antivirových databází do úložiště.

Krok 7. Definování názvu úlohy

Zadejte název úlohy, například `Denní úplná kontrola`.

Krok 8. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. V důsledku toho bude úloha Antivirová kontrola provedena v počítačích uživatelů podle určeného plánu.

[Jak vytvořit úlohu antivirové kontroly ve webové konzole]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   b. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Antivirová kontrola**.

   c. V poli **Název úlohy** zadejte krátký popis, například `Týdenní kontrola`.

   d. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Další**.

5. Kliknutím na tlačítko **Dokončit** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

6. Chcete-li nakonfigurovat plán úloh, přejděte do vlastností úloh.

   Doporučuje se nakonfigurovat plán, který spustí úlohu alespoň jednou týdně.

7. Zaškrtněte políčko vedle úlohy.

8. Klikněte na tlačítko **Spustit**.

   Můžete sledovat stav úlohy a počet zařízení, ve kterých byla úloha úspěšně dokončena nebo dokončena s chybou.

V důsledku toho bude úloha Antivirová kontrola provedena v počítačích uživatelů podle určeného plánu.

Správa zásad

Zásada je souhrn nastavení aplikace, která jsou definována pro skupinu pro správu. Pro jednu aplikaci můžete nakonfigurovat více zásad s různými hodnotami. Aplikaci lze spustit s různými nastaveními pro různé skupiny pro správu. Každá skupina pro správu může mít svou vlastní zásadu pro aplikaci.

Nastavení zásad jsou odeslána do klientských počítačů součástí Network Agent během *synchronizace*. Ve výchozím nastavení provádí server pro správu synchronizaci okamžitě po změně nastavení zásad. Pro synchronizaci se používá port UDP 15000 v klientském počítači. Server pro správu provádí synchronizaci každých 15 minut. Pokud se synchronizace po změně nastavení zásad nezdaří, další pokus o synchronizaci bude proveden podle nakonfigurovaného plánu.

Aktivní a neaktivní zásada

Zásada je určena pro skupinu spravovaných počítačů a může být aktivní nebo neaktivní. Nastavení aktivní zásady se během synchronizace uloží do klientských počítačů. Na jeden počítač nelze použít více zásad současně, a proto může být v každé skupině aktivní pouze jedna zásada.

Můžete vytvořit neomezený počet neaktivních zásad. Neaktivní zásada neovlivní nastavení aplikace v počítačích v síti. Neaktivní zásady jsou určeny jako přípravy pro nouzové situace, jako je útok viru. Pokud dojde k útoku přes jednotky flash, můžete aktivovat zásadu, která blokuje přístup k jednotkám flash. V tomto případě se aktivní zásada automaticky stane neaktivní.

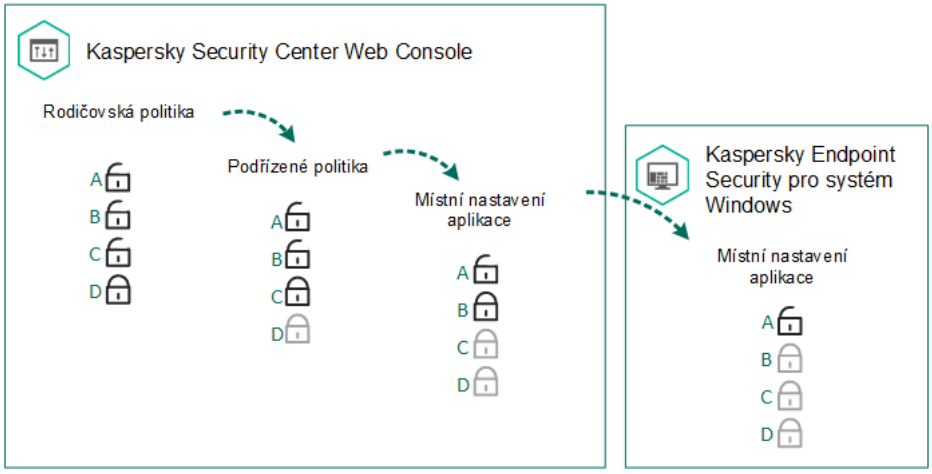
Zásada „mimo kancelář“

Zásada „mimo kancelář“ je aktivována v případě, že počítač opustí hranice sítě organizace.

Dědičnost nastavení

Zásady, jako jsou administrativní skupiny, jsou uspořádány v hierarchii. Ve výchozím nastavení podřízená zásada dědí nastavení z nadřazené zásady. *Podřízená zásada* je zásada pro vnořené úrovně hierarchie, což je zásada pro vnořené skupiny pro správu a sekundární servery pro správu. Dědičnost nastavení z nadřazené zásady můžete deaktivovat.

Nastavení každé zásady obsahuje atribut , který udává, zda lze toto nastavení upravit v podřízených zásadách nebo v místních nastaveních aplikace. Atribut je se používá pouze v případě, že je v podřízené zásadě povoleno dědění nastavení nadřazených zásad. Zásady pro uživatele mimo kancelář neovlivňují jiné zásady v rámci hierarchie skupin pro správu.



Dědičnost nastavení

Oprávnění pro přístup k nastavení zásad (čtení, zápis, spouštění) lze určit pro každého uživatele, který má přístup k administračnímu serveru Kaspersky Security Center, a samostatně pro každý funkční rozsah aplikace Kaspersky Endpoint Security. Chcete-li nakonfigurovat oprávnění pro přístup k nastavení zásad, přejděte do části **Security** v okně vlastností administračního serveru Kaspersky Security Center.

Vytvoření zásad

Jak vytvořit instalační zásadu v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu vyberte složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Klikněte na tlačítko **New policy**.

   Spustí se průvodce zásad.
5. Postupujte podle pokynů průvodce zásad.

Jak vytvořit zásadu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce zásad.
3. Vyberte aplikaci Kaspersky Endpoint Security a klikněte na tlačítko **Další**.
4. Přečtěte si a přijměte podmínky Prohlášení týkající se služby Kaspersky Security Network (KSN) a klikněte na tlačítko **Další**.
5. Na kartě **Obecné** můžete provést následující akce:
   - Změňte název zásady.
   - Vyberte stav zásady:
     - **Aktivní**. Po další synchronizaci bude zásada v počítači použita jako aktivní zásada.
     - **Neaktivní**. Slouží jako záložní zásada. V případě potřeby lze neaktivní zásadu přepnout do aktivního stavu.
     - **Mimo kancelář**. Zásada je aktivována v případě, že počítač opustí hranice sítě organizace.
   - Nakonfigurujte dědění nastavení:
     - **Dědit nastavení z nadřazené zásady**. Pokud je toto přepínací tlačítko v zapnutém stavu, hodnoty nastavení zásad jsou děděny ze zásady nejvyšší úrovně. Nastavení zásad nelze upravit, pokud je pro nadřazenou zásadu nastaven symbol .
     - **Vynutit dědění nastavení v podřízených zásadách**. Pokud je přepínací tlačítko v zapnutém stavu, hodnoty nastavení zásad jsou rozšířeny do podřízených zásad. Ve vlastnostech podřízených zásad se přepínací tlačítko **Zdědit nadřazené zásady zásad** automaticky zapne a nelze jej vypnout. Nastavení podřízených zásad jsou děděna z nadřazené zásady, kromě nastavení označených symbolem . Nastavení podřízených zásad nelze upravit, pokud je pro nadřazenou zásadu nastaven symbol .
6. Na kartě **Nastavení aplikace** můžete nakonfigurovat nastavení zásad aplikace Kaspersky Endpoint Security.
7. Klikněte na tlačítko **Uložit**.

V důsledku toho budou během další synchronizace v klientských počítačích nakonfigurovány zásady aplikace Kaspersky Endpoint Security. Informace o zásadách uplatňovaných v počítači můžete zobrazit v rozhraní aplikace Kaspersky Endpoint Security kliknutím na tlačítko **Podpora** na hlavní obrazovce (například název zásady). Chcete-li to provést, musíte v nastavení zásad součásti Network Agent povolit přijímání dat z rozšířených zásad. Další informace o zásadách součásti Network Agent najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

Ukazatel úrovně zabezpečení

Ukazatel úrovně zabezpečení se zobrazí v horní části okna **Properties: <Název zásady>**. Ukazatel může mít některou z následujících hodnot:

- **Vysoká úroveň ochrany**. Ukazatel má tuto hodnotu a jeho barva se změní na zelenou, pokud jsou povoleny všechny součásti z následujících kategorií:
  - **Kritické**. Tato kategorie obsahuje následující součásti:
    - Ochrana před souborovými hrozbami
    - Detekce chování
    - Prevence zneužití
    - Modul pro nápravu
  - **Důležité**. Tato kategorie obsahuje následující součásti:
    - Služba Kaspersky Security Network
    - Ochrana před webovými hrozbami
    - Ochrana před hrozbami v poště
    - Prevence narušení hostitele
- **Střední úroveň ochrany**. Ukazatel má tuto hodnotu a jeho barva se změní na žlutou, pokud je zakázána některá z důležitých součástí.
- **Nízká úroveň ochrany**. Ukazatel má tuto hodnotu a jeho barva se změní na červenou v některém z následujících případů:
  - Je zakázána jedna nebo více kritických součástí.
  - Jsou zakázány dvě nebo více důležitých součástí.

Pokud má ukazatel hodnotu **Střední úroveň ochrany** nebo **Nízká úroveň ochrany**, vpravo od něj se zobrazuje odkaz, který otevře okno **Doporučené součásti ochrany**. V tomto okně můžete povolit libovolné doporučené součásti ochrany.

Správa úloh

Můžete vytvářet následující typy úloh pro správu aplikace Kaspersky Endpoint Security prostřednictvím rozhraní Kaspersky Security Center:

- místní úlohy, které jsou nakonfigurovány pro jeden klientský počítač;
- skupinové úlohy, které jsou nakonfigurovány pro klientské počítače v rámci skupin správy;
- Úlohy pro výběr počítačů.

Můžete vytvořit libovolný počet skupinových úloh, úloh pro výběr počítačů nebo místních úloh. Podrobnější informace o práci se skupinami pro správu a výběru počítačů najdete v *nápovědě k aplikaci Kaspersky Security Center*.

Aplikace Kaspersky Endpoint Security podporuje následující úlohy:

- **Antivirová kontrola**. Aplikace Kaspersky Endpoint Security zkontroluje, zda se v oblastech počítače určených v nastavení úlohy nenacházejí viry či jiné hrozby. Úloha *Antivirová kontrola* je vyžadována pro fungování aplikace Kaspersky Endpoint Security a je vytvořena v průběhu Průvodce počáteční konfigurací. Doporučuje se nakonfigurovat plán, který spustí úlohu alespoň jednou týdně.

- **Přidat klíč**. Aplikace Kaspersky Endpoint Security přidá klíč pro aktivaci aplikací, včetně dalšího klíče. Před spuštěním úlohy se ujistěte, že počet počítačů, ve kterých má být úloha provedena, nepřekračuje počet počítačů povolený licencí.

- **Změnit součásti aplikace**. Aplikace Kaspersky Endpoint Security nainstaluje nebo odebere součásti v klientských počítačích na základě seznamu součástí uvedeného v nastavení úlohy. Součást Ochrana před souborovými hrozbami nelze odebrat. Optimální sada součástí aplikace Kaspersky Endpoint Security pomáhá šetřit prostředky počítače.

- **Inventarizace**. Aplikace Kaspersky Endpoint Security přijímá informace o všech spustitelných souborech aplikací, které jsou uloženy v počítačích. Úloha *Inventarizace* je provedena součástí Kontrola aplikací. Pokud součást Kontrola aplikací není nainstalována, úloha skončí chybou.

- **Aktualizace**. Aplikace Kaspersky Endpoint Security aktualizuje databáze a moduly aplikace. Úloha *Aktualizace* je vyžadována pro fungování aplikace Kaspersky Endpoint Security a je vytvořena v průběhu Průvodce počáteční konfigurací. Doporučuje se nakonfigurovat plán, který spustí úlohu alespoň jednou denně.

- **Vymazat data**. Aplikace Kaspersky Endpoint Security odstraní soubory a složky z počítačů uživatelů okamžitě nebo pokud po delší dobu nedojde k připojení k aplikaci Kaspersky Security Center.

- **Vrácení aktualizace zpět**. Aplikace Kaspersky Endpoint Security vrátí zpět poslední aktualizaci databází a modulů aplikace. To může být nezbytné například v případě, že nová databáze obsahuje nesprávná data, která mohou způsobit, že aplikace Kaspersky Endpoint Security zablokuje bezpečnou aplikaci.

- **Kontrola integrity**. Aplikace Kaspersky Endpoint Security analyzuje soubory aplikací, kontroluje poškození nebo změny souborů a ověřuje digitální podpisy souborů aplikací.

- **Správa účtů ověřovacího agenta**. Aplikace Kaspersky Endpoint Security konfiguruje nastavení účtu ověřovacího agenta. Pro práci se šifrovanými jednotkami je nutný ověřovací agent. Před načtením operačního systému musí uživatel dokončit ověření agentem.

Úlohy jsou spuštěny v počítači pouze v případě, že je spuštěna aplikace Kaspersky Endpoint Security.

Přidání nové úlohy

Jak vytvořit úlohu v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Vyberte složku **Tasks** ze stromu konzole pro správu.
3. Klikněte na tlačítko **Nová úloha**.
   Spustí se průvodce úlohou.
4. Postupujte podle pokynů průvodce úloh.

Jak vytvořit úlohu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   b. V rozevíracím seznamu **Typ úlohy** vyberte úlohu, kterou chcete spustit v počítačích uživatelů.

   c. V poli **Název úlohy** zadejte krátký popis, například `Aktualizace aplikace pro účetnictví`.

   d. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Další**.

5. Kliknutím na tlačítko **Dokončit** dokončete průvodce.

V seznamu úloh se zobrazí nová úloha. Úloha bude mít výchozí nastavení. Chcete-li nakonfigurovat nastavení úlohy, přejděte do vlastností úlohy. Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**. Po spuštění úlohy můžete úlohu pozastavit a obnovit ji později.

V seznamu úloh můžete sledovat výsledky úloh, které zahrnují stav úlohy a statistiky výkonu úloh v počítačích. Můžete také vytvořit výběr událostí a sledovat dokončení úloh (**Sledování a zprávy** → **Výběry událostí**). Další informace o výběru události najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*. Výsledky spuštění úlohy se uloží také místně v protokolu událostí systému Windows a ve zprávách aplikace Kaspersky Endpoint Security.

Řízení přístupu k úloze

Oprávnění pro přístup k aplikacím Kaspersky Endpoint Security (čtení, zápis, spouštění) lze definovat pro každého uživatele, který má přístup k administračnímu serveru Kaspersky Security Center, prostřednictvím nastavení přístupu k funkčním oblastem aplikace Kaspersky Endpoint Security. Chcete-li nakonfigurovat přístup k funkčním oblastem aplikace Kaspersky Endpoint Security, přejděte do části **Security** v okně vlastností administračního serveru Kaspersky Security Center. Podrobnější informace o správě úloh pomocí aplikace Kaspersky Security Center *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Oprávnění uživatelů pro přístup k úlohám můžete nakonfigurovat pomocí zásady (*režim správy úloh*). Můžete například skrýt úlohy skupiny v rozhraní aplikace Kaspersky Endpoint Security.

Jak nakonfigurovat režim správy úloh v rozhraní aplikace Kaspersky Endpoint Security pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Místní úlohy** → **Správa úloh**.
6. Nakonfigurujte režim správy úloh (viz tabulka níže).
7. Uložte změny.

Jak nakonfigurovat režim správy úloh v rozhraní aplikace Kaspersky Endpoint Security pomocí webové konzoly

1. V hlavním okně webové konzole vyberte kartu **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete povolit podporu mobilního režimu.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte na **Místní úlohy** → **Správa úloh**.
5. Nakonfigurujte režim správy úloh (viz tabulka níže).
6. Klikněte na tlačítko **OK**.
7. Potvrďte změny kliknutím na tlačítko **Uložit**.

Nastavení správy úloh

Parametr	Popis
Povolit použití místních úloh	Je-li toto políčko zaškrtnuto, místní úlohy se zobrazí v místním rozhraní aplikace Kaspersky Endpoint Security. Pokud neexistují žádná další omezení zásad, uživatel může úlohy nakonfigurovat a spustit. Konfigurace plánu spouštění úlohy však pro uživatele zůstává nedostupná. Uživatel může úlohy spouštět pouze ručně. Pokud toto políčko není zaškrtnuté, použití místních úloh je zastaveno. V tomto režimu se místní úlohy nespouští dle plánu. Úlohy nelze spustit ani nakonfigurovat v místním rozhraní aplikace Kaspersky Endpoint Security ani při práci s příkazovým řádkem. Uživatel může antivirovou kontrolu souboru nebo složky přesto spustit výběrem možnosti **Zkontrolovat na výskyt virů** v místní nabídce souboru nebo složky. Úloha kontroly se spustí s výchozími hodnotami nastavení pro vlastní Uživatelská kontrola.
Povolit zobrazení úloh skupiny	Je-li toto políčko zaškrtnuto, úlohy skupiny se zobrazí v místním rozhraní aplikace Kaspersky Endpoint Security. Uživatel si může zobrazit seznam všech úloh v rozhraní aplikace.

	Pokud políčko zaškrtnuto není, aplikace Kaspersky Endpoint Security zobrazí prázdný seznam úloh.
Povolit správu úloh skupiny	Pokud je políčko zaškrtnuté, uživatelé mohou spouštět a zastavovat úlohy skupiny uvedené v aplikaci Kaspersky Security Center. Uživatelé mohou spouštět a zastavovat úlohy v rozhraní aplikace nebo ve zjednodušeném rozhraní aplikace. Pokud políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security bude naplánované úlohy spouštět automaticky nebo správce bude úlohy spouštět ručně v aplikaci Kaspersky Security Center.

Konfigurace místních nastavení aplikace

V aplikaci Kaspersky Security Center můžete nakonfigurovat nastavení aplikace Kaspersky Endpoint Security v konkrétním počítači. Jedná se o *místní nastavení aplikace*. U některých zásad nemusí být k dispozici přístup k úpravám. Tato nastavení jsou zablokována atributem ve vlastnostech zásad.

Jak nakonfigurovat místní nastavení aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušný klientský počítač.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Vyberte počítač, pro který chcete konfigurovat nastavení aplikace Kaspersky Endpoint Security.
5. V kontextové nabídce klientského počítače vyberte možnost **Properties**.

   Otevře se okno vlastností klientského počítače.
6. V okně vlastností klientského počítače vyberte část **Applications**.

   V pravé části okna vlastností klientského počítače se zobrazí seznam aplikací společnosti Kaspersky, které jsou nainstalovány v klientském počítači.
7. Vyberte aplikaci Kaspersky Endpoint Security.
8. Klikněte na tlačítko **Properties** v seznamu aplikací Kaspersky.

   Otevře se okno **Kaspersky Endpoint Security for Windows application settings**.
9. V části **Obecná nastavení** můžete měnit nastavení aplikace Kaspersky Endpoint Security a také nastavení zpráv a úložiště.

   Ostatní části okna **Nastavení aplikace Kaspersky Endpoint Security pro systém Windows** jsou stejné jako ve standardních částech aplikace Kaspersky Security Center. Popis těchto částí je obsažen v nápovědě k aplikaci Kaspersky Security Center.

   > Pokud aplikace podléhá zásadám zakazujícím změny konkrétních nastavení, nebudete je moci při konfiguraci nastavení aplikace v části **Obecná nastavení** měnit.
10. Chcete-li uložit změny, v okně **Kaspersky Endpoint Security for Windows application settings** klikněte na tlačítko **OK**.

Jak nakonfigurovat místní nastavení aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Aplikace**.
4. Klikněte na možnost **Kaspersky Endpoint Security pro systém Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Nastavení aplikace**.
6. Nakonfigurujte místní nastavení aplikace.
7. Místní nastavení aplikace jsou stejná jako nastavení zásad s výjimkou nastavení šifrování.

Spuštění a zastavení aplikace Kaspersky Endpoint Security

Po instalaci aplikace Kaspersky Endpoint Security do počítače uživatele se aplikace automaticky spustí. Aplikace Kaspersky Endpoint Security se ve výchozím nastavení spustí po spuštění operačního systému. V nastavení operačního systému není možné nakonfigurovat automatické spouštění aplikace.

Stažení antivirových databází aplikace Kaspersky Endpoint Security po spuštění operačního systému může v závislosti na možnostech počítače trvat až dvě minuty. Během této doby je úroveň ochrany počítače snížena. Stahování antivirových databází, když je aplikace Kaspersky Endpoint Security spuštěna v již spuštěném operačním systému, nezpůsobuje snížení úrovně ochrany počítače.

Jak nakonfigurovat spouštění aplikace Kaspersky Endpoint Security v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Obecná nastavení** → **Nastavení aplikace**.
6. Pomocí zaškrtávacího políčka **Spouštět Kaspersky Endpoint Security pro systém Windows při spuštění počítače** nakonfigurujte spuštění počítače.
7. Uložte změny.

Jak nakonfigurovat spouštění aplikace Kaspersky Endpoint Security ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. U počítačů, pro které chcete nakonfigurovat spuštění aplikace, klikněte na název zásady aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte **Obecná nastavení**.
5. Klikněte na odkaz **Nastavení aplikace**.
6. Pomocí zaškrtávacího políčka **Spouštět Kaspersky Endpoint Security pro systém Windows při spuštění počítače** nakonfigurujte spuštění počítače.
7. Klikněte na tlačítko **OK**.
8. Potvrďte změny kliknutím na tlačítko **Uložit**.

Jak nakonfigurovat spuštění aplikace Kaspersky Endpoint Security v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Obecné**.
3. Pomocí zaškrtávacího políčka **Spustit při spuštění počítače** nakonfigurujte, jak se má aplikace spouštět.
4. Změny uložíte kliknutím na tlačítko **Uložit**.

Odborníci společnosti Kaspersky nedoporučují zastavovat aplikaci Kaspersky Endpoint Security ručně, protože tím počítač a svá osobní data vystavíte hrozbám. V případě nutnosti můžete ochranu počítače pozastavit na libovolnou dobu, aniž by došlo k zastavení aplikace.

Stav aplikace můžete sledovat pomocí widgetu **Stav ochrany**.

Jak spustit nebo zastavit aplikaci Kaspersky Endpoint Security v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušný klientský počítač.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Vyberte počítač, ve kterém chcete aplikaci spustit nebo zastavit.
5. Kliknutím pravým tlačítkem myši zobrazte kontextovou nabídku klientského počítače a vyberte položku **Properties**.
6. V okně vlastností klientského počítače vyberte část **Applications**.

   V pravé části okna vlastností klientského počítače se zobrazí seznam aplikací společnosti Kaspersky, které jsou nainstalovány v klientském počítači.
7. Vyberte aplikaci Kaspersky Endpoint Security.
8. Postupujte následovně:
   - Aplikaci spustíte kliknutím na tlačítko  na pravé straně seznamu aplikací společnosti Kaspersky.
   - Aplikaci zastavíte kliknutím na tlačítko  na pravé straně seznamu aplikací společnosti Kaspersky.

Jak spustit nebo zastavit aplikaci Kaspersky Endpoint Security ve webové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Klikněte na název počítače, ve kterém chcete spustit nebo zastavit aplikaci Kaspersky Endpoint Security.

   Otevře se okno vlastností počítače.
3. Vyberte kartu **Aplikace**.
4. Zaškrtněte políčko u aplikace **Kaspersky Endpoint Security pro systém Windows**.
5. Klikněte na tlačítko **Start** nebo **Zastavit**.

Jak spustit nebo zastavit aplikaci Kaspersky Endpoint Security z příkazového řádku

Chcete-li zastavit aplikaci z příkazového řádku, povolte externí správu systémových služeb.

Soubor klpsm.exe, který je součástí distribučního balíčku aplikace Kaspersky Endpoint Security, slouží ke spuštění nebo k zastavení aplikace z příkazového řádku.

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.
3. Chcete-li spustit aplikaci z příkazového řádku, zadejte `klpsm.exe start_avp_service`.
4. Chcete-li zastavit aplikaci z příkazového řádku, zadejte `klpsm.exe stop_avp_service`.

Pozastavení a obnovení ochrany a kontroly počítače

Pozastavení ochrany a kontroly počítače znamená zakázání všech součástí ochrany a kontroly aplikace Kaspersky Endpoint Security.

Stav aplikace lze zobrazit pomocí ikony aplikace v oznamovací oblasti hlavního panelu.

- Ikona značí, že ochrana a kontrola počítače je pozastavena.
- Ikona značí, že ochrana a kontrola počítače je aktivována.

Pozastavení nebo obnovení ochrany a kontroly počítače nemá vliv na úlohy kontroly nebo aktualizace.

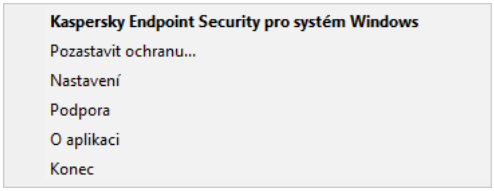
Pokud jsou v době pozastavení nebo obnovení ochrany a kontroly počítače navázána nějaká síťová připojení, zobrazí se upozornění na ukončení těchto síťových připojení.

Pozastavení ochrany a kontroly počítače:

1. Kliknutím pravým tlačítkem myši na ikonu aplikace v oznamovací oblasti hlavního panelu otevřete kontextovou nabídku.
2. V kontextové nabídce vyberte položku **Pozastavit ochranu** (viz obrázek níže).

   Tato položka místní nabídky je k dispozici, pokud je aktivována ochrana heslem.
3. Vyberte jednu z následujících možností:
   - **Pozastavit na <doba>** – ochrana a kontrola počítače se obnoví po době zadané v rozevíracím seznamu níže.
   - **Pozastavit do restartování aplikace** – ochrana a kontrola počítače se obnoví po restartování aplikace nebo po restartování systému. Aby bylo možné tuto možnost použít, musí být povoleno automatické spuštění aplikace.
   - **Pozastavit** – ochrana a kontrola počítače se obnoví poté, co ji znovu povolíte.
4. Klikněte na tlačítko **Pozastavit ochranu**.

Kaspersky Endpoint Security pozastaví činnost všech součástí ochrany a kontroly, které nejsou v zásadách označeny zámkem (). Před provedením této operace doporučujeme zakázat zásady aplikace Kaspersky Security Center.



Kontextová nabídka ikony Aplikace

Obnovení ochrany a kontroly počítače:

1. Kliknutím pravým tlačítkem myši na ikonu aplikace v oznamovací oblasti hlavního panelu otevřete kontextovou nabídku.

2. V kontextové nabídce vyberte položku **Obnovit ochranu**.

Ochranu a kontrolu počítače můžete kdykoli obnovit bez ohledu na možnost pozastavení ochrany a kontroly počítače, kterou jste předtím vybrali.

Kontrola počítače

Antivirová kontrola je zásadní pro bezpečnost počítače. Pravidelně provádějte antivirovou kontrolu, abyste zabránili šíření malwaru, který nebyl zjištěn součástmi ochrany z důvodu nízkého nastavení úrovně zabezpečení nebo z jiných důvodů.

Aplikace Kaspersky Endpoint Security nekontroluje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive, a vytváří položky protokolu, které uvádějí, že tyto soubory nebyly prohledány.

Úplná kontrola

Důkladně zkontroluje celý počítač. Aplikace Kaspersky Endpoint Security kontroluje tyto objekty:

- paměť jádra;
- objekty načítané při spouštění operačního systému;
- spouštěcí sektory;
- zálohu operačního systému;
- všechny pevné disky a vyměnitelné jednotky.

Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Úplná kontrola*.

Chcete-li ušetřit prostředky počítače, místo úlohy úplné kontroly se doporučuje spustit úlohu kontroly na pozadí. Neovlivní to úroveň zabezpečení počítače.

Kontrola kritických oblastí

Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků.

Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Kontrola kritických oblastí*.

Vlastní kontrola

Aplikace Kaspersky Endpoint Security kontroluje objekty, které vybral uživatel. Můžete kontrolovat kterýkoli objekt na tomto seznamu:

- paměť jádra;
- objekty načítané při spouštění operačního systému;
- zálohu operačního systému;

- Poštovní schránka aplikace Outlook;
- pevné, vyměnitelné a síťové jednotky;
- jakýkoli vybraný soubor.

Kontrola na pozadí

Kontrola na pozadí je režim kontroly aplikace Kaspersky Endpoint Security, který uživateli nezobrazuje oznámení. Kontrola na pozadí vyžaduje méně prostředků počítače než jiné typy kontrol (například úplná kontrola). V tomto režimu aplikace Kaspersky Endpoint Security kontroluje spouštěcí objekty, spouštěcí sektor, systémovou paměť a systémový oddíl.

Kontrola integrity

Aplikace Kaspersky Endpoint Security zkontroluje moduly aplikace z hlediska změn nebo poškození.

Spuštění nebo zastavení úlohy kontroly

Bez ohledu na vybraný režim spuštění úlohy kontroly můžete úlohu kontroly kdykoli spustit nebo zastavit.

Postup spuštění nebo zastavení úlohy kontroly:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. Chcete-li spustit úlohu kontroly, klikněte na tlačítko **Zahájit kontrolu**.

   Aplikace Kaspersky Endpoint Security spustí kontrolu počítače. Aplikace zobrazí průběh kontroly, počet zkontrolovaných souborů a zbývající čas kontroly. Úlohu můžete kdykoli zastavit kliknutím na tlačítko **Zastavit**.

Postup spuštění nebo zastavení úlohy kontroly v případě zobrazení zjednodušeného rozhraní aplikace:

1. Kliknutím pravým tlačítkem myši na ikonu aplikace v oznamovací oblasti hlavního panelu otevřete kontextovou nabídku.
2. V rozevíracím seznamu **Úlohy** v kontextové nabídce proveďte jednu z následujících akcí:
   - Vyberte nespuštěnou úlohu kontroly a spusťte ji.
   - Vyberte spuštěnou úlohu kontroly a zastavte ji.
   - Vyberte pozastavenou úlohu kontroly a obnovte ji nebo ji spusťte znovu.

Změna úrovně zabezpečení

Aplikace Kaspersky Endpoint Security může pro spuštění kontroly použít různé skupiny nastavení. Tyto skupiny nastavení uložené v aplikaci se nazývají *úrovně zabezpečení*: **Vysoká**, **Doporučená**, **Nízká**. **Doporučená** nastavení úrovně zabezpečení jsou považována za optimální. Doporučují je odborníci společnosti Kaspersky. Můžete vybrat jednu z předvoleb úrovně zabezpečení nebo konfigurovat nastavení úrovně zabezpečení ručně. Pokud změníte nastavení úrovně zabezpečení, můžete se kdykoli vrátit zpět k doporučeným nastavením.

Postup změny úrovně zabezpečení:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. V části **Úroveň zabezpečení** proveďte některou z následujících akcí:
   - Chcete-li použít jednu z předvoleb úrovně zabezpečení, vyberte ji pomocí posuvníku:
     - **Vysoká**. Aplikace Kaspersky Endpoint Security kontroluje všechny typy souborů. Při kontrole složených souborů může aplikace Kaspersky Endpoint Security kontrolovat i soubory formátu e-mailu.
     - **Doporučená**. Aplikace Kaspersky Endpoint Security kontroluje pouze vybrané formáty souborů na všech pevných discích, síťových discích a vyměnitelných úložných médiích počítače a také vložené objekty OLE. Aplikace Kaspersky Endpoint Security nekontroluje archivy ani instalační balíčky.
     - **Nízká**. Aplikace Kaspersky Endpoint Security kontroluje pouze nové nebo upravené soubory s vybranými příponami na všech pevných discích, vyměnitelných jednotkách a síťových discích počítače. Aplikace Kaspersky Endpoint Security nekontroluje složené soubory.
   - Pokud chcete nakonfigurovat vlastní úroveň zabezpečení, klikněte na tlačítko **rozšířené nastavení** a definujte vlastní nastavení součásti.

     Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Obnovit doporučenou úroveň zabezpečení** v horní části okna.
4. Uložte změny.

Změna akce, která se má provést s infikovanými soubory

Ve výchozím nastavení se aplikace Kaspersky Endpoint Security při zjištění infikovaných souborů pokusí tyto soubory dezinfikovat nebo je odstraní (pokud není dezinfekce možná).

Postup změny akce, která se má provést s infikovanými soubory:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. V bloku **Akce při zjištění hrozby** vyberte některou z následujících možností:
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní.
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory.

Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.

- **Informovat**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb.

Před pokusem o dezinfekci nebo odstranění infikovaného souboru vytvoří aplikace Kaspersky Endpoint Security záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.

Při zjištění infikovaných souborů, které jsou součástí aplikace ze služby Windows Store, se aplikace Kaspersky Endpoint Security pokusí soubor odstranit.

4. Uložte změny.

Vygenerování seznamu objektů ke kontrole

Vygenerování seznamu objektů ke kontrole:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Klikněte na odkaz **Upravit rozsah kontroly**.
4. V okně, které se otevře, vyberte objekty, které chcete přidat do rozsahu kontroly nebo z něj vyloučit.

   Objekty, které jsou ve výchozím rozsahu kontroly, nelze odebírat ani upravovat.

5. Pokud chcete do rozsahu kontroly přidat nový objekt:

   a. Klikněte na tlačítko **Přidat**.

   Otevře se strom složek.

   b. Vyberte objekt a klikněte na tlačítko **Vybrat**.

   Objekt můžete z kontroly vyloučit, aniž byste jej odstranili ze seznamu objektů v rozsahu kontroly. Chcete-li tak učinit, zrušte zaškrtnutí políčka vedle objektu.

6. Uložte změny.

Výběr typu souborů ke kontrole

Při volbě typů souborů ke kontrole mějte na paměti následující informace:

1. Existuje nízká pravděpodobnost zavedení škodlivého kódu do souborů určitých formátů a jeho následné aktivace (například formát TXT). Existují však některé formáty souborů, které obsahují spustitelný kód (např. .exe, .dll nebo .doc). Spustitelný kód mohou také obsahovat soubory formátů, které nejsou pro tento účel určeny (například formát DOC). U těchto souborů je riziko narušení pomocí škodlivého kódu a jeho aktivace velké.

2. Narušitel může odeslat virus nebo jinou škodlivou aplikaci do počítače ve formě spustitelného souboru, který je přejmenovaný a má příponu .txt. Pokud vyberete kontrolu souborů podle přípony, aplikace při kontrole takový soubor přeskočí. Pokud je vybrána kontrola souborů podle formátu, aplikace Kaspersky Endpoint Security analyzuje záhlaví souboru bez ohledu na příponu. Pokud tato analýza odhalí, že soubor má formát spustitelného souboru (například EXE), aplikace jej zkontroluje.

Postup výběru typu souborů ke kontrole:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.

2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V části **Typy souborů** zadejte typ souborů, který chcete při spuštění vybrané úlohy kontroly kontrolovat:

   - **Všechny soubory**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje všechny soubory bez výjimky (všechny formáty a přípony).

   - **Soubory kontrolované podle formátu**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami.

   - **Soubory kontrolované podle přípony**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.

   Aplikace Kaspersky Endpoint Security považuje soubory bez přípony za spustitelné soubory. Aplikace Kaspersky Endpoint Security vždy kontroluje spustitelné soubory, bez ohledu na typy souborů, které pro kontrolu vyberete.

5. Uložte změny.

Optimalizace kontroly souborů

Kontrolu souborů můžete optimalizovat: zkrátit dobu trvání kontroly a zvýšit rychlost operací aplikace Kaspersky Endpoint Security. Toho lze dosáhnout tak, že budou kontrolovány jen nové soubory a soubory, které byly od předchozí kontroly změněny. Tento režim se vztahuje jak na jednoduché, tak na složené soubory. Také můžete nastavit limit pro kontrolu jednoho souboru. Jakmile určený časový interval vyprší, aplikace Kaspersky Endpoint Security soubor vyloučí z aktuální kontroly (s výjimkou archivů a objektů obsahujících více souborů).

Můžete také povolit použití technologií iChecker a iSwift. Technologie iChechker a iSwift optimalizují rychlost kontroly souborů tím, že jsou vyloučeny soubory, které nebyly od poslední kontroly změněny.

Postup optimalizace kontroly souborů:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.

2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V bloku **Optimalizace kontroly** nakonfigurujte nastavení kontroly:

   - **Kontrolovat pouze nové a změněné soubory**. Kontroluje pouze nové soubory a soubory, které byly od posledního skenování změněny. To pomáhá zkrátit dobu skenování. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.

   - **Přeskočit soubory, které se kontrolují déle než N sekund**. Omezí dobu trvání kontroly jednoho objektu. Po zadané době aplikace Kaspersky Endpoint Security ukončí kontrolu souboru. To pomáhá zkrátit dobu skenování.

5. Uložte změny.

Kontrola složených souborů

Častou technikou ukrývání virů a jiného malwaru je jejich implantace do složených souborů, jakými jsou archivy či databáze. Aby bylo možné zjistit viry a jiný malware skrytý tímto způsobem, složený soubor musí být rozbalen, což může zpomalit kontrolu. Typy kontrolovaných složených souborů můžete omezit a tím kontrolu urychlit.

Postup konfigurace kontroly složených souborů:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.

2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V části **Kontrola složených souborů** určete, které složené soubory chcete kontrolovat: archivy, instalační balíčky, soubory kancelářských dokumentů, soubory e-mailů a heslem chráněné archivy.

5. Pokud je zakázána kontrola pouze nových a upravených souborů, nakonfigurujte nastavení pro kontrolu každého typu složeného souboru: kontrolovat všechny soubory tohoto typu nebo pouze nové soubory.

   Pokud je povolena kontrola pouze nových a upravených souborů, Kaspersky Endpoint Security kontroluje pouze nové a upravené soubory všech typů složených souborů.

6. V bloku **Omezení velikosti** proveďte jednu z následujících akcí:

   - Pokud nechcete, aby byly rozbalovány velké složené soubory, zaškrtněte políčko **Nerozbalovat velké složené soubory** a zadejte požadovanou hodnotu do pole **Maximální velikost souboru**.

   - Pokud chcete, aby byly složené soubory rozbalovány bez ohledu na velikost, zrušte zaškrtnutí políčka **Nerozbalovat velké složené soubory**.

   Aplikace Kaspersky Endpoint Security kontroluje velké soubory extrahované z archivů bez ohledu na to, zda je či není zaškrtnuto políčko **Nerozbalovat velké složené soubory**.

7. Uložte změny.

Použití metod kontroly

Aplikace Kaspersky Endpoint Security používá metodu kontroly zvanou strojové učení a analýza signatur. Během analýzy podle databází páruje aplikace Kaspersky Endpoint Security zjištěné objekty se záznamy v databázi. Na základě doporučení odborníků společnosti Kaspersky je metoda strojového učení a analýzy signatur vždy povolena.

Chcete-li zvýšit účinnost ochrany, můžete použít heuristickou analýzu. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.

Použití metod kontroly:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Pokud chcete, aby aplikace pro spuštění úlohy kontroly používala heuristickou analýzu, v bloku **Metody kontroly** zaškrtněte políčko **Heuristická analýza**. Poté pomocí posuvníku nastavte úroveň heuristické analýzy: **Lehká kontrola**, **Střední kontrola** nebo **Hloubková kontrola**.
5. Uložte změny.

Použití technologií

Použití technologií kontroly:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Technologie kontroly** zaškrtněte políčka vedle názvů technologií, které chcete použít během kontroly.

   - **Technologie iSwift**. Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.

   - **Technologie iChecker**. Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).

5. Uložte změny.

Volba režimu spuštění úlohy kontroly

Pokud z jakéhokoli důvodu nelze úlohu kontroly spustit (například, když je počítač vypnutý), můžete nakonfigurovat automatické spuštění vynechané úlohy ihned, jakmile to bude možné.

Pokud se čas zahájení kontroly shoduje s časem spuštění aplikace Kaspersky Endpoint Security, můžete spuštění úlohy kontroly odložit po spuštění aplikace. Úloha kontroly může být spuštěna pouze po uplynutí určeného časového intervalu od spuštění aplikace Kaspersky Endpoint Security.

Volba režimu spuštění úlohy kontroly:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Klikněte na tlačítko **Plán kontrol**.
4. V okně, které se otevře, nakonfigurujte plán spuštění úlohy kontroly.
5. V závislosti na vybrané frekvenci proveďte rozšířené nastavení pro plán spouštění úlohy.
   a. Pokud chcete, aby aplikace Kaspersky Endpoint Security spouštěla neprovedené úlohy kontroly při první příležitosti, zaškrtněte políčko **Spustit plánovanou kontrolu následující den, pokud bude počítač vypnutý**.

      Pokud je v rozevíracím seznamu **Spouštět kontrolu** vybrána možnost **Každou minutu**, **Každou hodinu**, **Po spuštění aplikace** nebo **Po každé aktualizaci**, zaškrtávací políčko **Spustit plánovanou kontrolu následující den, pokud bude počítač vypnutý** není k dispozici.

   b. Chcete-li, aby aplikace Kaspersky Endpoint Security pozastavila úlohu, když má počítač k dispozici omezené prostředky, zaškrtněte políčko **Spustit pouze v době, kdy je počítač neaktivní**. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky.

      Tato možnost plánu šetří prostředky počítače.
6. Uložte změny.

Spuštění úlohy kontroly pod jiným uživatelským účtem

Úloha kontroly je ve výchozím nastavení spuštěna s oprávněními účtu, ke kterému je uživatel přihlášený v operačním systému. Může se však stát, že budete potřebovat spustit úlohu kontroly s jiným uživatelským účtem. Můžete zadat uživatele, který má vhodná práva v nastavení úlohy kontroly, a úlohu kontroly spustit pod účtem tohoto uživatele.

Postup konfigurace spuštění úlohy kontroly pod jiným uživatelským účtem:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Klikněte na možnosti **Rozšířené nastavení** → **Spustit kontrolu jako**.

4. V okně, které se otevře, vyberte uživatele, který vyžaduje práva ke spuštění úlohy kontroly.

5. Uložte změny.

Kontrola vyměnitelných jednotek připojených k počítači

Kaspersky Endpoint Security kontroluje všechny soubory, které spouštíte nebo kopírujete, i když je soubor umístěn na vyměnitelné jednotce (součást Ochrana před souborovými hrozbami). Abyste zabránili šíření virů a dalšího malwaru, můžete nakonfigurovat automatické kontroly vyměnitelných jednotek při připojení k počítači. Aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. Tato součást chrání počítač prováděním kontrol, které implementují strojové učení, heuristickou analýzu (na vysoké úrovni) a analýzu podpisů. Kaspersky Endpoint Security rovněž používá technologie pro optimalizaci kontroly iSwift a iChecker. Tyto technologie jsou vždy zapnuté a nelze je vypnout.

Postup konfigurace kontroly vyměnitelných jednotek připojených k počítači:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.

2. V okně, které se otevře, vyberte úlohu kontroly vyměnitelné jednotky a klikněte na tlačítko ⚙.

3. Pomocí přepínače **Kontrola vyměnitelných jednotek** můžete povolit nebo zakázat kontrolu vyměnitelných jednotek po připojení k počítači.

4. Vyberte režim pro kontrolu vyměnitelných jednotek při připojení:

   - **Podrobná kontrola** Je-li vybrána tato možnost, při připojení vyměnitelné jednotky aplikace Kaspersky Endpoint Security zkontroluje všechny soubory, které se nachází na vyměnitelné jednotce, včetně souborů integrovaných ve složených objektech, archivů, distribučních balíčků a souborů v kancelářských formátech. Kaspersky Endpoint Security nekontroluje soubory ve formátu pošty ani archivy chráněné heslem.

   - **Rychlá kontrola** Je-li tato možnost vybrána, po připojení vyměnitelné jednotky aplikace Kaspersky Endpoint Security zkontroluje pouze soubory v konkrétních formátech, které jsou na infekce nejnáchylnější, a nerozbalí složené objekty.

5. Pokud chcete, aby aplikace Kaspersky Endpoint Security kontrolovala jen vyměnitelné jednotky o velikosti nepřekračující zadanou hodnotu, zaškrtněte políčko **Maximální velikost vyměnitelné jednotky** a do sousedícího pole zadejte hodnotu (v megabajtech).

6. Nakonfigurujte, jak se bude zobrazovat průběh kontroly vyměnitelného disku. Proveďte jednu z následujících akcí:

   - Chcete-li, aby aplikace Kaspersky Endpoint Security zobrazila průběh kontroly vyměnitelné jednotky v samostatném okně, zaškrtněte políčko **Zobrazit průběh kontroly**.

     V okně kontroly vyměnitelné jednotky může uživatel kontrolu zastavit. Chcete-li, aby kontrola byla povinná a uživatel ji nemohl zastavit, zaškrtněte políčko **Blokovat zastavení úlohy kontroly**.

   - Chcete-li, aby aplikace Kaspersky Endpoint Security spouštěla kontrolu vyměnitelných jednotek na pozadí, zrušte zaškrtnutí políčka **Zobrazit průběh kontroly**.

7. Změny uložíte kliknutím na tlačítko **Uložit**.

Kontrola na pozadí

Kontrola na pozadí je režim kontroly aplikace Kaspersky Endpoint Security, který uživateli nezobrazuje oznámení. Kontrola na pozadí vyžaduje méně prostředků počítače než jiné typy kontrol (například úplná kontrola). V tomto režimu aplikace Kaspersky Endpoint Security kontroluje spouštěcí objekty, spouštěcí sektor, systémovou paměť a systémový oddíl. Kontrola na pozadí se spustí v následujících případech:

- Po dokončení aktualizace antivirové databáze.
- 30 minut po spuštění aplikace Kaspersky Endpoint Security.
- Každých šest hodin.
- Když je počítač nečinný po dobu pěti nebo více minut (počítač je uzamčen nebo je zapnutý spořič obrazovky).

Testování na pozadí, když je počítač nečinný, je přerušeno, pokud jsou splněny některé z následujících podmínek:

- Počítač přešel do aktivního režimu.

  Pokud skenování na pozadí nebylo spuštěno déle než deset dní, skenování nebude přerušeno.

- Počítač (notebook) se přepnul do režimu napájení z baterie.

Při provádění kontroly na pozadí aplikace Kaspersky Endpoint Security nekontroluje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive.

Povolení kontroly na pozadí v počítači:

1. V hlavním okně aplikace klikněte na tlačítko **Úlohy**.
2. V okně, které se otevře, vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Pomocí přepínače **Kontrola na pozadí** povolte nebo zakažte kontroly na pozadí.
4. Uložte změny.

Kontrola integrity modulů aplikace

Aplikace Kaspersky Endpoint Security kontroluje, zda u souborů aplikace v instalační složce aplikace nedošlo ke změnám nebo poškození. Pokud má například knihovna aplikace nesprávný digitální podpis, je považována za poškozenou. Úloha *Kontrola integrity* je určena ke kontrole souborů aplikací. Úlohu *Kontrola integrity* spusťte, pokud aplikace Kaspersky Endpoint Security zjistila škodlivý objekt, ale neneutralizovala ho.

Úlohu *Kontrola integrity* můžete vytvořit jak ve webové konzole aplikace Kaspersky Security Center 12, tak v konzole pro správu. Tuto úlohu nelze vytvořit v cloudové konzole Kaspersky Security Center.

[Jak provést kontrolu integrity aplikace prostřednictvím konzoly pro správu (MMC)]

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

   Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnosti **Kaspersky Endpoint Security pro systém Windows (11.6.0)** → **Kontrola integrity**.

Krok 2. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 3. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán pro spuštění úlohy, například ručně nebo při zjištění virové epidemie.

Krok 4. Definování názvu úlohy

Zadejte název úlohy, například `Kontrola integrity po infikování počítače`.

Krok 5. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. Kaspersky Endpoint Security zkontroluje integritu aplikace. Případně můžete ve vlastnostech úlohy nakonfigurovat plán kontroly integrity aplikace.

[Jak provést kontrolu integrity aplikace prostřednictvím webové konzoly]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   b. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Kontrola integrity**.

   c. Do pole **Název úlohy** zadejte stručný popis, například `Kontrola integrity aplikace po infekci počítače`.

   d. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Další**.

5. Kliknutím na tlačítko **Dokončit** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

6. Zaškrtněte políčko vedle úlohy.

Kaspersky Endpoint Security zkontroluje integritu aplikace. Případně můžete ve vlastnostech úlohy nakonfigurovat plán kontroly integrity aplikace.

K porušení integrity aplikace může dojít v následujících případech:

- Škodlivý objekt změnil soubory aplikace Kaspersky Endpoint Security. V takovém případě proveďte postup obnovení aplikace Kaspersky Endpoint Security pomocí nástrojů operačního systému. Po obnovení spusťte úplnou kontrolu počítače a zopakujte kontrolu integrity.
- Platnost digitálního podpisu skončila. V takovém případě aktualizujte aplikaci Kaspersky Endpoint Security.

Aktualizace databází a softwarových modulů aplikace

Aktualizace databází a modulů aplikace Kaspersky Endpoint Security zajišťuje maximální ochranu počítače. Nové viry a jiné typy malwaru se objevují po celém světě každý den. Databáze aplikace Kaspersky Endpoint Security obsahují informace o hrozbách a možnostech jejich zneškodnění. Pro rychlou detekci hrozeb je důležité, aby byly databáze a moduly aplikace pravidelně aktualizovány.

Pravidelné aktualizace vyžadují platnou licenci. Pokud nemáte k dispozici žádnou licenci, aktualizaci budete moci provést jen jednou.

Hlavním zdrojem aktualizací pro aplikaci Kaspersky Endpoint Security jsou aktualizační servery společnosti Kaspersky.

Aby bylo možné stáhnout z aktualizačních serverů společnosti Kaspersky balíčky aktualizací, počítač musí být připojený k internetu. Nastavení připojení k internetu je ve výchozím nastavení určováno automaticky. Pokud používáte proxy server, musíte konfigurovat jeho nastavení.

Aktualizace se stahují přes protokol HTTPS. Když není možné aktualizace stahovat přes protokol HTTPS, mohou se také stahovat přes protokol HTTP.

Při provádění aktualizace jsou do počítače staženy a nainstalovány následující objekty:

- Databáze aplikace Kaspersky Endpoint Security. Ochrana počítače je zajišťována pomocí databází, které obsahují podpisy virů a jiných hrozeb a informace o tom, jak je lze zneškodnit. Součásti ochrany tyto informace používají při hledání a zneškodňování infikovaných souborů v počítači. Databáze jsou neustále aktualizovány záznamy o nových hrozbách a způsobech jejich zneškodnění. Proto je doporučujeme aktualizovat pravidelně.

  Kromě databází aplikace Kaspersky Endpoint Security jsou také aktualizovány síťové ovladače, které umožňují součástem aplikace zachytit síťový provoz.

- Moduly aplikace. Kromě databází aplikace Kaspersky Endpoint Security můžete aktualizovat také moduly aplikace. Aktualizace modulů aplikace opravuje zranitelnosti v aplikaci Kaspersky Endpoint Security, přidává nové funkce nebo vylepšuje ty stávající.

Moduly aplikace a databáze v počítači jsou při aktualizaci porovnávány s aktuální verzí ve zdroji aktualizace. Pokud se vaše současné databáze a moduly aplikace liší od příslušných aktuálních verzí, do počítače se nainstalují chybějící části aktualizace.

S aktualizací modulů aplikace lze aktualizovat všechny soubory kontextové nápovědy.

Pokud jsou databáze zastaralé, balíček aktualizace může být velký, což může způsobit dodatečný internetový provoz (až několik desítek MB).

Informace o aktuálním stavu databází aplikace Kaspersky Endpoint Security se zobrazí v části **Aktualizace** v okně **Úlohy**.

Informace o výsledcích aktualizace a všech událostech, k nimž dojde během aktualizace, jsou zaznamenávány do zprávy aplikace Kaspersky Endpoint Security.

Scénáře aktualizace databázového a aplikačního modulu

Aktualizace databází a modulů aplikace Kaspersky Endpoint Security zajišťuje maximální ochranu počítače. Nové viry a jiné typy malwaru se objevují po celém světě každý den. Databáze aplikace Kaspersky Endpoint Security obsahují informace o hrozbách a možnostech jejich zneškodnění. Pro rychlou detekci hrozeb je důležité, aby byly databáze a moduly aplikace pravidelně aktualizovány.

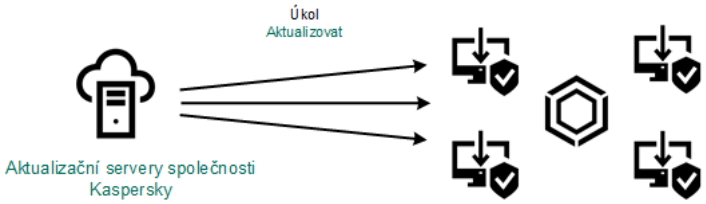
V počítačích uživatelů se aktualizují následující objekty:

- Antivirové databáze. Antivirové databáze obsahují databáze signatur malwaru, popis síťových útoků, databáze škodlivých a phishingových webových adres, databáze reklamních lišt, databáze nevyžádané pošty a další data.
- Moduly aplikace. Aktualizace modulů jsou určeny k odstranění slabých míst v aplikaci a ke zlepšení způsobů ochrany počítače. Aktualizace modulů mohou změnit chování součástí aplikace a přidat nové možnosti.

Aplikace Kaspersky Endpoint Security podporuje následující scénáře aktualizace databází a modulů aplikace:

- Aktualizace ze serverů společnosti Kaspersky.

  Aktualizační servery společnosti Kaspersky jsou umístěny v různých zemích po celém světě. Tím je zajištěna vysoká spolehlivost aktualizací. Pokud nelze provést aktualizaci z jednoho serveru, aplikace Kaspersky Endpoint Security přejde na další server.



Aktualizace ze serverů společnosti Kaspersky.

- Centralizovaná aktualizace.

  Centralizovaná aktualizace snižuje externí internetový provoz a zajišťuje pohodlné sledování aktualizace.

  Centralizovaná aktualizace se skládá z následujících kroků:

  1. Stáhněte aktualizační balíček do úložiště v síti organizace.

     Balíček aktualizace je stažen do úložiště pomocí úlohy serveru pro správu s názvem *Stažení aktualizací do úložiště serveru pro správu*.

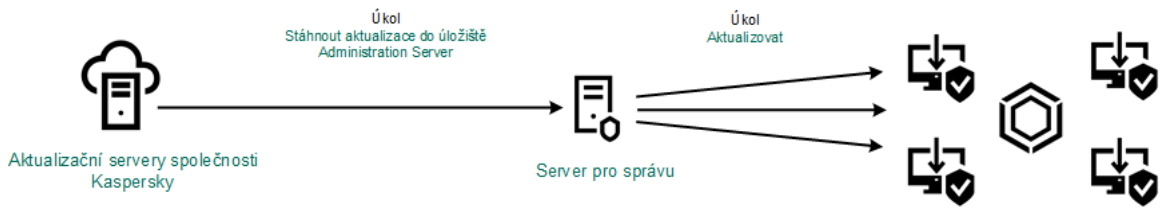
  2. Stáhněte balíček aktualizace do sdílené složky (volitelné).

     Balíček aktualizace můžete do úložiště stáhnout následujícími způsoby:

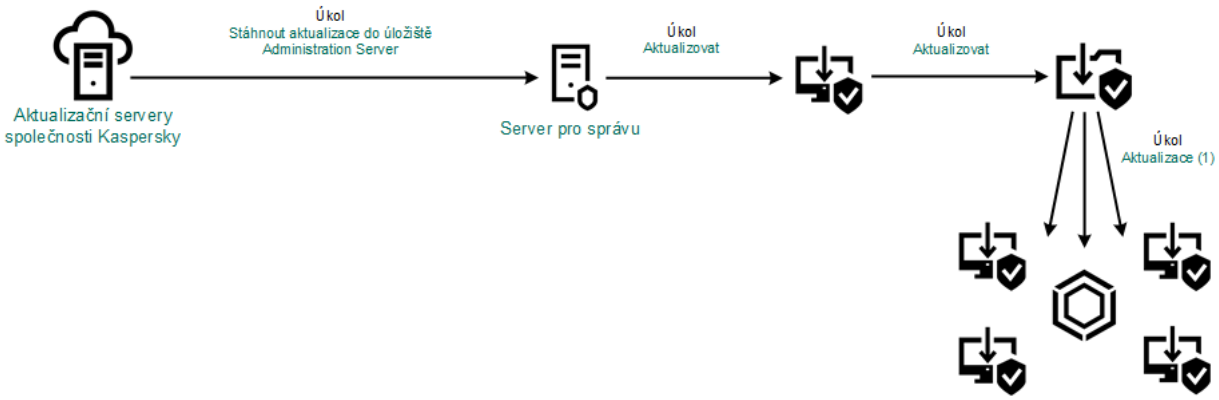
     - Pomocí úlohy *Aktualizace* v aplikaci Kaspersky Endpoint Security. Úloha je určena pro některý z počítačů v místní firemní síti.
     - Pomocí nástroje Kaspersky Update Utility. Podrobné informace o použití nástroje Kaspersky Update Utility *najdete ve znalostní bázi společnosti Kaspersky*.

  3. Proveďte distribuci aktualizačního balíčku do klientských počítačů.

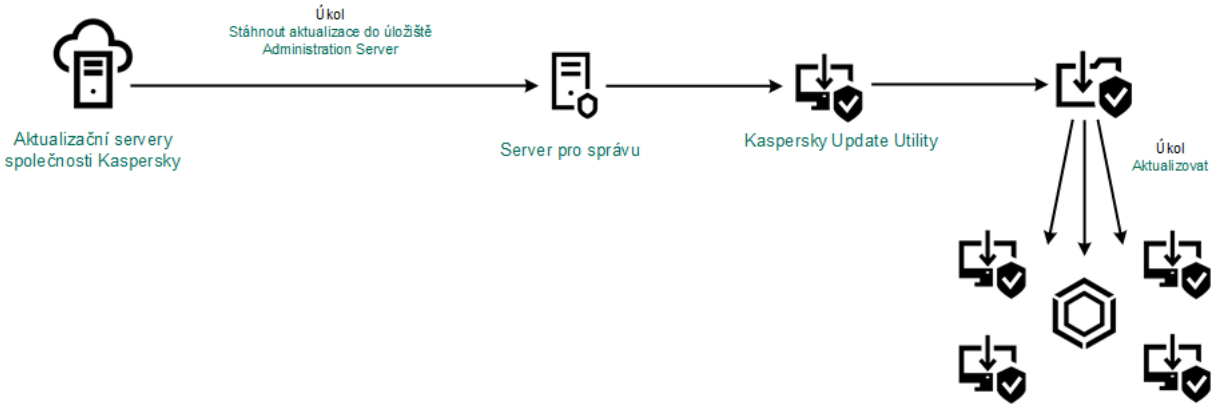
     Aktualizační balíček je distribuován do klientských počítačů pomocí úlohy *Aktualizace* v aplikaci Kaspersky Endpoint Security. Můžete vytvořit neomezený počet úloh aktualizací pro každou skupinu správy.



Aktualizace ze serverového úložiště



Aktualizace ze sdílené složky



Aktualizace pomocí nástroje Kaspersky Update Utility

U webové konzoly výchozí seznam zdrojů aktualizací obsahuje server pro správu aplikace Kaspersky Security Center a aktualizační servery společnosti Kaspersky. U cloudové konzole aplikace Kaspersky Security Center obsahuje výchozí seznam zdrojů aktualizace distribuční body a aktualizační servery společnosti Kaspersky. Další informace o distribučních bodech najdete v *nápovědě ke cloudové konzole aplikace Kaspersky Security Center*. Do seznamu můžete přidat další zdroje aktualizací. Jako zdroje aktualizací můžete určit servery HTTP/FTP a sdílené složky. Pokud nelze provést aktualizaci ze zdroje aktualizací, aplikace Kaspersky Endpoint Security přejde na další zdroj.

Aktualizace jsou staženy z aktualizačních serverů společnosti Kaspersky nebo z jiných serverů FTP či HTTP přes standardní síťové protokoly. Pokud je pro přístup ke zdroji aktualizace vyžadováno připojení k proxy serveru, určete nastavení proxy serveru v nastaveních zásad aplikace Kaspersky Endpoint Security.

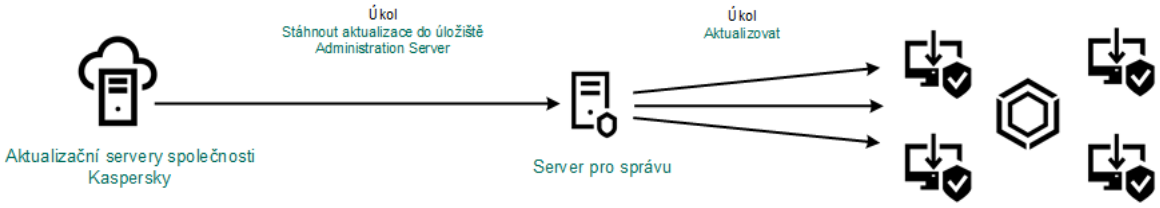
Aktualizace ze serverového úložiště

Chcete-li šetřit internetový provoz, můžete nakonfigurovat aktualizace databází a modulů aplikace v počítačích v síti LAN organizace ze serverového úložiště. Za tímto účelem musí aplikace Kaspersky Security Center stáhnout aktualizační balíček do úložiště (server FTP nebo HTTP, síťová nebo místní složka) z aktualizačních serverů společnosti Kaspersky. Další počítače v síti LAN organizace budou moci obdržet aktualizační balíček ze serverového úložiště.

Konfigurace aktualizací databází a modulů aplikace ze serverového úložiště se skládá z následujících kroků:

1. Nakonfigurujte stažení aktualizačního balíčku do úložiště serveru pro správu (úloha *Stažení aktualizací do úložiště serveru pro správu*).

2. Nakonfigurujte aktualizace databází a modulů aplikace z určeného serverového úložiště do zbývajících počítačů v síti LAN organizace (úloha *Aktualizace*).



Aktualizace ze serverového úložiště

Postup konfigurace stažení aktualizačního balíčku do serverového úložiště:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Vyberte úlohu serveru pro správu **Stažení aktualizací do úložiště**.

   Otevře se okno vlastností úlohy.

   Úloha serveru pro správu *Stáhnout aktualizace do úložiště* je automaticky vytvořena Průvodcem počáteční konfigurací Kaspersky Security Center 12 Web Console a tato úloha může mít pouze jednu instanci.

3. Vyberte kartu **Nastavení aplikace**.

4. V části **Další nastavení** klikněte na tlačítko **Konfigurovat**.

5. V poli **Aktualizovat složku úložiště** zadejte adresu serveru FTP nebo HTTP, síťové složky nebo místní složky, kam aplikace Kaspersky Security Center zkopíruje aktualizační balíček přijatý z aktualizačních serverů společnosti Kaspersky.

   Pro zdroj aktualizací se používá následující formát cesty:

   - Pro server FTP nebo HTTP zadejte jeho webovou adresu nebo IP adresu.

     Například `http://dnl-01.geo.kaspersky.com/` nebo `93.191.13.103`.

     Pro server FTP můžete zadat nastavení ověřování v adrese v následujícím formátu: `ftp://<uživatelské jméno>:<heslo>@<hostitel>:<port>`

   - U síťové složky zadejte cestu UNC.

     Například: `\\ Server\Share\Update distribution`.

   - U síťové nebo místní složky zadejte úplnou cestu ke složce.

     Například `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Uložte změny.

Postup konfigurace aktualizace aplikace Kaspersky Endpoint Security z určeného webového úložiště:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Aktualizace** pro aplikaci Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

Úloha *Aktualizace* je automaticky vytvořena průvodcem počáteční konfigurací aplikace Kaspersky Security Center. Chcete-li vytvořit úlohu *Aktualizace*, nainstalujte při spuštění průvodce webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Nastavení aplikace** → **Místní režim**.
4. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.
5. V poli **Zdroj** zadejte adresu serveru FTP nebo HTTP, síťové složky nebo místní složky, kam aplikace Kaspersky Security Center zkopíruje aktualizační balíček přijatý ze serverů společnosti Kaspersky.

   Adresa zdroje aktualizace se musí shodovat s adresou zadanou v poli **Složka pro uložení aktualizací** při konfiguraci stažení aktualizací do serverového úložiště (viz *výše uvedené pokyny*).

6. V části **Stav** vyberte možnost **Povoleno**.
7. Klikněte na tlačítko **OK**.
8. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.
9. Klikněte na tlačítko **Uložit**.

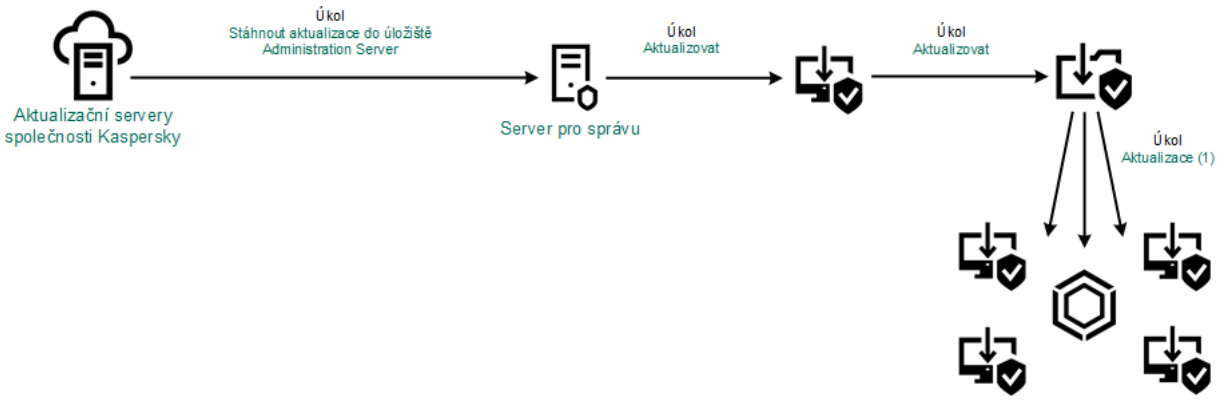
Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

Aktualizace ze sdílené složky

Chcete-li šetřit internetový provoz, můžete nakonfigurovat aktualizace databází a modulů aplikace v počítačích v síti LAN organizace ze sdílené složky. Za tímto účelem musí jeden z počítačů v síti LAN organizace obdržet aktualizační balíčky ze serveru pro správu aplikace Kaspersky Security Center nebo z aktualizačních serverů společnosti Kaspersky a zkopíruje je do sdílené složky. Další počítače v síti LAN organizace budou moci obdržet aktualizační balíček z této sdílené složky.

Konfigurace aktualizací databází a modulů aplikace ze sdílené složky se skládá z následujících kroků:

1. Konfigurace aktualizací modulů databází a aplikací z úložiště serveru.
2. Povolení zkopírování aktualizačního balíčku do sdílené složky v jednom z počítačů místní sítě LAN (viz pokyny níže).
3. Konfigurace aktualizací databází a modulů aplikace z určené sdílené složky do zbývajících počítačů v podnikové síti LAN (viz pokyny níže).



Postup povolení kopírování aktualizačního balíčku do sdílené složky:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Aktualizace** pro aplikaci Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace* je automaticky vytvořena průvodcem počáteční konfigurací aplikace Kaspersky Security Center. Chcete-li vytvořit úlohu *Aktualizace*, nainstalujte při spuštění průvodce webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Nastavení aplikace** → **Místní režim**.

4. Nakonfigurujte zdroje aktualizací.

   Mezi zdroje aktualizací mohou patřit aktualizační servery společnosti Kaspersky, server pro správu aplikace Kaspersky Security Center, další servery FTP nebo HTTP, místní složky nebo síťové složky.

5. Zaškrtněte políčko **Zkopírovat aktualizace do složky**.

6. Do pole **Cesta** zadejte cestu UNC ke sdílené složce (například `\\Server\Share\Update distribution`).

   Pokud je políčko ponecháno prázdné, aplikace Kaspersky Endpoint Security zkopíruje aktualizační balíček do složky `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

7. Klikněte na tlačítko **Uložit**.

Úlohu *Aktualizace* je nutné přiřadit k jednomu počítači, který bude sloužit jako zdroj aktualizací.

Postup konfigurace aktualizací ze sdílené složky:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   b. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Aktualizace**.

   c. V poli **Název úlohy** zadejte krátký popis, například `Aktualizace ze sdílené složky`.

   d. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

      Úlohu *Aktualizace* je nutné přiřadit k počítačům v síti LAN organizace, kromě počítače, který slouží jako zdroj aktualizací.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy a klikněte na tlačítko **Další**.
5. Kliknutím na tlačítko **Vytvořit** dokončete průvodce.

   V tabulce úloh se zobrazí nová úloha.
6. Klikněte na nově vytvořenou úlohu *Aktualizace*.

   Otevře se okno vlastností úlohy.
7. Přejděte do části **Nastavení aplikace**.
8. Vyberte kartu **Místní režim**.
9. V části **Zdroj aktualizací** klikněte na tlačítko **Přidat**.
10. V poli **Zdroj** zadejte cestu ke sdílené složce.

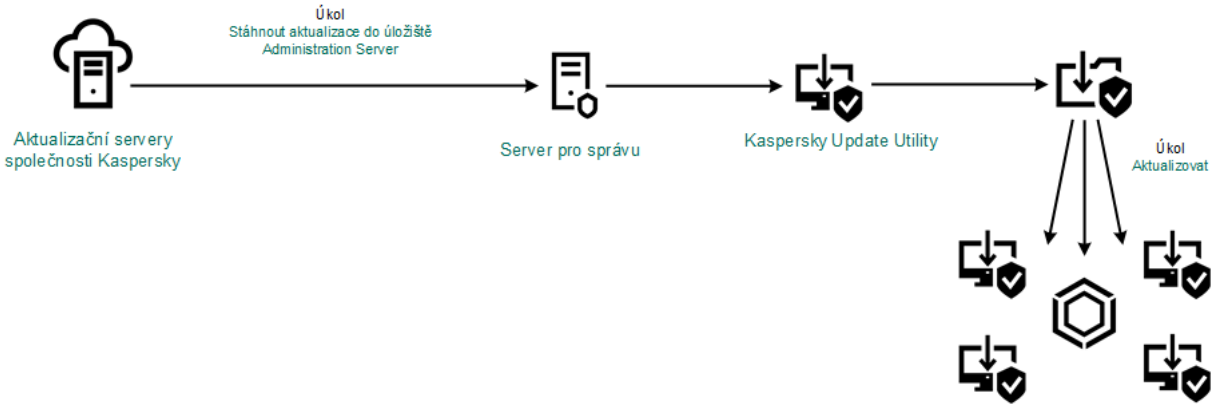
    Zdrojová adresa se musí shodovat s adresou, kterou jste dříve zadali v poli **Cesta** při konfiguraci kopírování balíčku aktualizace do sdílené složky (viz *výše uvedené pokyny*).
11. Klikněte na tlačítko **OK**.
12. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.
13. Klikněte na tlačítko **Uložit**.

Aktualizace pomocí nástroje Kaspersky Update Utility

Chcete-li šetřit internetový provoz, můžete nakonfigurovat aktualizace databází a modulů aplikace v počítačích v síti LAN organizace ze sdílené složky pomocí nástroje Kaspersky Update Utility. Za tímto účelem musí jeden z počítačů v síti LAN organizace obdržet aktualizační balíčky ze serveru pro správu aplikace Kaspersky Security Center nebo z aktualizačních serverů společnosti Kaspersky a pomocí uvedeného nástroje je zkopíruje do sdílené složky. Další počítače v síti LAN organizace budou moci obdržet aktualizační balíček z této sdílené složky.

Konfigurace aktualizací databází a modulů aplikace ze sdílené složky se skládá z následujících kroků:

1. Konfigurace aktualizací modulů databází a aplikací z úložiště serveru.
2. Nainstalujte nástroj Kaspersky Update Utility do jednoho z počítačů v síti LAN organizace.
3. V nastavení nástroje Kaspersky Update Utility nakonfigurujte kopírování balíčku aktualizace do sdílené složky.
4. Konfigurace aktualizací databází a modulů aplikace z určené sdílené složky do zbývajících počítačů v síti LAN organizace.



Aktualizace pomocí nástroje Kaspersky Update Utility

Distribuční balíček nástroje Kaspersky Update Utility si můžete stáhnout z webové stránky technické podpory společnosti Kaspersky. Po instalaci nástroje vyberte zdroj aktualizace (například úložiště serveru pro správu) a sdílenou složku, do které nástroj Kaspersky Update Utility zkopíruje balíčky aktualizací. Podrobné informace o použití nástroje Kaspersky Update Utility *najdete ve znalostní bázi společnosti Kaspersky*.

Postup konfigurace aktualizací ze sdílené složky:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Aktualizace** pro aplikaci Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace* je automaticky vytvořena průvodcem počáteční konfigurací aplikace Kaspersky Security Center. Chcete-li vytvořit úlohu *Aktualizace*, nainstalujte při spuštění průvodce webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Nastavení aplikace** → **Místní režim**.

4. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.

5. Do pole **Zdroj** zadejte cestu UNC ke sdílené složce (například `\\Server\Share\Update distribution`).

   Zdrojová adresa se musí shodovat s adresou uvedenou v nastavení nástroje Kaspersky Update Utility.

6. Klikněte na tlačítko **OK**.

7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

8. Klikněte na tlačítko **Uložit**.

Aktualizace v mobilním režimu

Mobilní režim je režim fungování aplikace Kaspersky Endpoint Security, kdy počítač opustí hranice sítě organizace (*počítač v režimu offline*). Podrobnější informace o práci s počítači v režimu offline a s uživateli mimo kancelář *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Počítač v režimu offline mimo síť organizace se nemůže připojit k serveru pro správu, aby aktualizoval databáze a moduly aplikace. Ve výchozím nastavení jsou jako zdroj aktualizace pro aktualizaci databází a modulů aplikací v mobilním režimu použity pouze aktualizační servery společnosti Kaspersky. Použití proxy serveru pro připojení k internetu je určeno zvláštní zásadou „mimo kancelář“. Zásadu „mimo kancelář“ je nutné vytvořit samostatně. Když je aplikace Kaspersky Endpoint Security přepnuta do mobilního režimu, úloha aktualizace se spustí každé dvě hodiny.

Postup konfigurace nastavení aktualizace pro mobilní režim:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Aktualizace** pro aplikaci Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace* je automaticky vytvořena průvodcem počáteční konfigurací aplikace Kaspersky Security Center. Chcete-li vytvořit úlohu *Aktualizace*, nainstalujte při spuštění průvodce webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

   Vyberte kartu **Nastavení aplikace** → **Mobilní režim**.

3. Nakonfigurujte zdroje aktualizací. Mezi zdroje aktualizací mohou patřit aktualizační servery společnosti Kaspersky, další servery FTP a HTTP, místní složky nebo síťové složky.

4. Klikněte na tlačítko **Uložit**.

V důsledku toho budou databáze a moduly aplikace aktualizovány v počítačích uživatelů po jejich přepnutí do mobilního režimu.

Spuštění a zastavení úlohy aktualizace

Bez ohledu na vybraný režim spuštění úlohy můžete úlohu aktualizace aplikace Kaspersky Endpoint Security kdykoli spustit nebo zastavit.

Postup spuštění nebo zastavení úlohy aktualizace:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.

2. Chcete-li spustit úlohu aktualizace, v bloku **Aktualizace databází a modulů aplikace** klikněte na tlačítko **Aktualizovat**.

Aplikace Kaspersky Endpoint Security začne aktualizovat moduly a databáze aplikace. Aplikace zobrazí průběh úlohy, velikost stažených souborů a zdroj aktualizace. Chcete-li tuto úlohu zastavit, kdykoli můžete kliknout na tlačítko .

Postup spuštění nebo zastavení úlohy aktualizace v případě zobrazení zjednodušeného rozhraní aplikace:

1. Kliknutím pravým tlačítkem myši na ikonu aplikace v oznamovací oblasti hlavního panelu otevřete kontextovou nabídku.

2. V rozevíracím seznamu **Úlohy** v kontextové nabídce proveďte jednu z následujících akcí:

   - Vyberte nespuštěnou úlohu aktualizace a spusťte ji.
   - Vyberte spuštěnou úlohu aktualizace a zastavte ji.

- Vyberte pozastavenou úlohu aktualizace a obnovte ji nebo ji spusťte znovu.

Spuštění úlohy aktualizace za použití oprávnění jiného uživatelského účtu

Ve výchozím nastavení je úloha aktualizace aplikace Kaspersky Endpoint Security spuštěna jménem uživatele, jehož účet byl použit k přihlášení do operačního systému. Aplikace Kaspersky Endpoint Security však může být aktualizována ze zdroje, ke kterému nemá uživatel přístup kvůli nedostatečným oprávněním (například sdílená složka obsahující balíček aktualizace), nebo ze zdroje, u kterého není nakonfigurováno ověření proxy serveru. V nastavení Kaspersky Endpoint Security můžete určit uživatele, který potřebná oprávnění má, a spustit úlohu aktualizace aplikace Kaspersky Endpoint Security v rámci účtu tohoto uživatele.

Postup spuštění úlohy aktualizace pomocí jiného uživatelského účtu:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.
2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.
3. Klikněte na tlačítko **Nastavení uživatelského účtu**.
4. V okně, které se otevře, vyberte možnost **Spustit aktualizace databází s uživatelskými oprávněními**.
5. Zadejte přihlašovací údaje k účtu uživatele s potřebnými oprávněními pro přístup ke zdroji aktualizace.
6. Uložte změny.

Volba režimu spuštění úlohy aktualizace

Pokud z jakéhokoli důvodu nelze úlohu aktualizace spustit (například, když je počítač vypnutý), můžete nakonfigurovat automatické spuštění vynechané úlohy ihned, jakmile to bude možné.

Spuštění úlohy aktualizace můžete odložit po spuštění aplikace, pokud pro úlohu aktualizace zvolíte režim spuštění **Podle plánu** a pokud se čas spuštění aplikace Kaspersky Endpoint Security shoduje s plánem spuštění úlohy aktualizace. Úloha aktualizace může být spuštěna pouze po uplynutí určeného časového intervalu od spuštění aplikace Kaspersky Endpoint Security.

Volba režimu spuštění úlohy aktualizace:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.
2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.
3. Klikněte na tlačítko **Nastavit režim aktualizace databází**.
4. V okně, které se otevře, vyberte režim spuštění úlohy aktualizace:

   - Pokud chcete, aby aplikace Kaspersky Endpoint Security spouštěla úlohy aktualizace podle toho, zda je ve zdroji aktualizací k dispozici balíček aktualizace, vyberte položku **Automaticky**. Četnost kontrol dostupnosti balíčků aktualizací prováděných aplikací Kaspersky Endpoint Security je během virových epidemií vyšší.

- Pokud chcete spouštět úlohy aktualizace ručně, vyberte položku **Ručně**.
- Chcete-li konfigurovat pro úlohu aktualizace plán spouštění, vyberte položku <**Podle plánu**>. Konfigurace rozšířeného nastavení pro spuštění úlohy aktualizace:
  - V poli **Odložit spuštění úlohy po startu aplikace o** zadejte časový interval pro spuštění úlohy aktualizace poté, co se spustí aplikace Kaspersky Endpoint Security.
  - Pokud chcete, aby aplikace Kaspersky Endpoint Security co nejdříve spustila úlohy aktualizace, které byly vynechány, zaškrtněte políčko **Spustit neprovedené úlohy**.

5. Uložte změny.

Přidání zdroje aktualizací

Zdroj aktualizací je prostředek, který obsahuje aktualizace pro databáze a moduly aplikace Kaspersky Endpoint Security.

Zdroje aktualizací zahrnují server aplikace Kaspersky Security Center, aktualizační servery společnosti Kaspersky a síťové nebo místní složky.

Výchozí seznam zdrojů aktualizací zahrnuje aplikaci Kaspersky Security Center a aktualizační servery společnosti Kaspersky. Do seznamu můžete přidat další zdroje aktualizací. Jako zdroje aktualizací můžete určit servery HTTP/FTP a sdílené složky.

Aplikace Kaspersky Endpoint Security nepodporuje aktualizace ze serverů HTTPS, pokud nejde o aktualizační servery společnosti Kaspersky.

Pokud je více prostředků vybráno jako zdroje aktualizací, aplikace Kaspersky Endpoint Security se pokusí o postupné připojení ke každému z nich, počínaje od začátku seznamu, a provede úlohu aktualizace získáním aktualizačního balíčku z prvního dostupného zdroje.

Postup přidání zdroje aktualizací:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.
2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.
3. Klikněte na tlačítko **Vybrat zdroje aktualizací**.
4. V daném okně klikněte na tlačítko **Přidat**.
5. V okně, které se otevře, zadejte adresu serveru FTP nebo HTTP, síťové složky nebo místní složky, která obsahuje balíček aktualizace.

   Pro zdroj aktualizací se používá následující formát cesty:

   - Pro server FTP nebo HTTP zadejte jeho webovou adresu nebo IP adresu.

     Například `http://dnl-01.geo.kaspersky.com/` nebo `93.191.13.103`.

     Pro server FTP můžete zadat nastavení ověřování v adrese v následujícím formátu: `ftp://<uživatelské jméno>:<heslo>@<hostitel>:<port>`

- U síťové složky zadejte cestu UNC.

  Například: `\\ Server\Share\Update distribution`.

- U síťové nebo místní složky zadejte úplnou cestu ke složce.

  Například `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Klikněte na tlačítko **Vybrat**.
7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.
8. Uložte změny.

Konfigurace aktualizací ze sdílené složky

Chcete-li šetřit internetový provoz, můžete nakonfigurovat aktualizace databází a modulů aplikace v počítačích v síti LAN organizace ze sdílené složky. Za tímto účelem musí jeden z počítačů v síti LAN organizace obdržet aktualizační balíčky ze serveru pro správu aplikace Kaspersky Security Center nebo z aktualizačních serverů společnosti Kaspersky a zkopíruje je do sdílené složky. Další počítače v síti LAN organizace budou moci obdržet aktualizační balíček z této sdílené složky.

Konfigurace aktualizací databází a modulů aplikace ze sdílené složky se skládá z následujících kroků:

1. Povolení zkopírování aktualizačního balíčku do sdílené složky v jednom z počítačů místní sítě.
2. Konfigurace aktualizací databází a modulů aplikace z určené sdílené složky do zbývajících počítačů v síti LAN organizace.

Postup povolení kopírování aktualizačního balíčku do sdílené složky:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.
2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.
3. V bloku **Distribuce aktualizací** zaškrtněte políčko **Zkopírovat aktualizace do složky**.
4. Zadejte cestu UNC ke sdílené složce (například `\\Server\Share\Update distribution`).
5. Uložte změny.

Postup konfigurace aktualizací ze sdílené složky:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.
2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.
3. Klikněte na tlačítko **Vybrat zdroje aktualizací**.
4. V daném okně klikněte na tlačítko **Přidat**.

5. V okně, které se otevře, zadejte cestu ke sdílené složce.

   Zdrojová adresa se musí shodovat s adresou, kterou jste dříve zadali při konfiguraci kopírování balíčku aktualizace do sdílené složky (viz *výše uvedené pokyny*).

6. Klikněte na tlačítko **Vybrat**.

7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

8. Uložte změny.

Aktualizace modulů aplikace

Aktualizace modulů aplikace opravují chyby, zlepšují výkon a přidávají nové funkce. Jakmile bude k dispozici nová aktualizace modulu aplikace, musíte potvrdit instalaci aktualizace. Instalaci aktualizace modulu aplikace můžete potvrdit buď v rozhraní aplikace, nebo v aplikaci Kaspersky Security Center. Jakmile bude k dispozici aktualizace, aplikace Kaspersky Endpoint Security zobrazí v hlavním okně aplikace jedno z následujících oznámení: důležitá aktualizace () nebo kritická aktualizace (). Pokud aktualizace modulu aplikace vyžadují kontrolu a přijetí podmínek Licenční smlouvy s koncovým uživatelem, aplikace nainstaluje aktualizace po přijetí podmínek Licenční smlouvy s koncovým uživatelem. Podrobnosti o sledování aktualizací modulů aplikace a potvrzení aktualizace v aplikaci Kaspersky Security Center *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Po instalaci aktualizace aplikace může být nutné restartovat počítač.

Postup konfigurace aktualizací modulů aplikace:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.

2. Vyberte úlohu *Aktualizovat* a klikněte na odkaz **Režim spuštění: <režim>**.

   Otevřou se vlastnosti úlohy *aktualizace*.

3. V bloku **Stahování a instalace aktualizací modulů aplikace** zaškrtněte políčko **Stáhnout aktualizace modulů aplikace**.

4. Vyberte aktualizace aplikačního modulu, které chcete nainstalovat.

   - **Instalovat důležité a schválené aktualizace**. Pokud je tato možnost vybrána, když jsou dostupné aktualizace modulu aplikace, aplikace Kaspersky Endpoint Security nainstaluje automaticky důležité aktualizace a všechny ostatní aktualizace modulu aplikace až poté, co bude jejich instalace schválena místně prostřednictvím rozhraní aplikace nebo ze strany služby Kaspersky Security Center.

   - **Instalovat pouze schválené aktualizace**. Pokud je tato možnost vybrána, když jsou dostupné aktualizace modulu aplikace, aplikace Kaspersky Endpoint Security je nainstaluje až poté, co bude jejich instalace schválena místně prostřednictvím rozhraní aplikace nebo ze strany služby Kaspersky Security Center. Tato možnost je nastavena jako výchozí.

5. Uložte změny.

Použití proxy serveru pro aktualizace

Abyste mohli stáhnout aktualizace databáze a modulů aplikace ze zdroje aktualizace, může být vyžadováno určení nastavení proxy serveru. Pokud je k dispozici více zdrojů aktualizací, nastavení proxy serveru jsou použita na všechny zdroje. Pokud není proxy server pro některé zdroje aktualizací třeba, můžete zakázat použití serveru proxy ve vlastnostech zásad. Aplikace Kaspersky Endpoint Security bude také používat proxy server pro přístup k síti Kaspersky Security Network a aktivačním serverům.

Postup konfigurace připojení ke zdrojům aktualizace pomocí proxy serveru:

1. V hlavním okně webové konzole klikněte na ikonu .

   Otevře se okno vlastností administračního serveru.

2. Přejděte do části **Nastavení přístupu k internetu**.

3. Zaškrtněte políčko **Použít proxy server**.

4. Nakonfigurujte nastavení připojení proxy serveru: adresa proxy serveru, port a nastavení ověřování (uživatelské jméno a heslo).

5. Klikněte na tlačítko **Uložit**.

Postup zakázání použití proxy serveru pro konkrétní skupinu pro správu:

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.

2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete zakázat použití proxy serveru.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Nastavení aplikace**.

4. Přejděte do části **Obecná nastavení** → **Nastavení sítě**.

5. V části **Nastavení proxy serveru** vyberte možnost **Nepoužívat proxy server**.

6. Klikněte na tlačítko **OK**.

7. Potvrďte změny kliknutím na tlačítko **Uložit**.

Postup konfigurace nastavení proxy serveru v rozhraní aplikace:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V bloku **Proxy server** klikněte na odkaz **Nastavení proxy serveru**.

4. V okně, které se otevře, vyberte jednu z následujících možností určení adresy proxy serveru:

   - **Automaticky zjistit nastavení proxy serveru**.

     Tato možnost je nastavena jako výchozí. Aplikace Kaspersky Endpoint Security používá nastavení proxy serveru, která jsou definována v nastavení operačního systému.

- **Použít zadaná nastavení proxy serveru**.

  Pokud jste vybrali tuto možnost, nakonfigurujte nastavení pro připojení k proxy serveru: adresa proxy serveru a port.

5. Pokud chcete povolit ověřování na proxy serveru, zaškrtněte políčko **Použít autorizaci proxy serveru** a zadejte přihlašovací údaje ke svému uživatelskému účtu.

6. Chcete-li zakázat použití proxy serveru při aktualizaci databází a modulů aplikace ze sdílené složky, zaškrtněte políčko **Nepoužívat proxy server pro adresy vnitřní sítě**.

7. Uložte změny.

Aplikace Kaspersky Endpoint Security tak bude používat proxy server ke stahování aktualizací modulů a databází aplikace. Aplikace Kaspersky Endpoint Security bude také používat proxy server pro přístup k serverům KSN a aktivačním serverům. Pokud je na proxy serveru vyžadováno ověření, ale nebyly zadány přihlašovací údaje k uživatelskému účtu nebo jsou nesprávné, aplikace Kaspersky Endpoint Security vás vyzve k zadání uživatelského jména a hesla.

Vrácení změn provedených poslední aktualizací

Po první aktualizaci databází a modulů aplikace bude k dispozici funkce obnovení předchozích verzí databází a modulů aplikace.

Pokaždé, když uživatel spustí proces aktualizace, vytvoří aplikace Kaspersky Endpoint Security záložní kopii aktuálních databází a modulů aplikace. To umožňuje v případě potřeby obnovit předchozí verze databází a modulů aplikace. Vrácení poslední aktualizace je užitečné například tehdy, když nová verze databáze obsahuje neplatný podpis, který způsobí, že aplikace Kaspersky Endpoint Security zablokuje bezpečnou aplikaci.

Postup vrácení poslední aktualizace:

1. V hlavním okně aplikace klikněte na tlačítko **Aktualizace databáze**.

2. V bloku **Vrácení databází k předchozí verzi** klikněte na tlačítko **Vrátit zpět**.

Aplikace Kaspersky Endpoint Security začne vracet poslední aktualizaci databáze. Aplikace zobrazí průběh vrácení, velikost stažených souborů a zdroj aktualizace. Chcete-li tuto úlohu zastavit, kdykoli můžete kliknout na tlačítko  .

Postup spuštění nebo zastavení úlohy vrácení akce zpět v případě zobrazení zjednodušeného rozhraní aplikace:

1. Kliknutím pravým tlačítkem myši na ikonu aplikace v oznamovací oblasti hlavního panelu otevřete kontextovou nabídku.

2. V rozevíracím seznamu **Úlohy** v kontextové nabídce proveďte jednu z následujících akcí:

   - Vyberte nespuštěnou úlohu vrácení akce zpět a zastavte ji.

   - Vyberte spuštěnou úlohu vrácení akce zpět a zastavte ji.

   - Vyberte pozastavenou úlohu vrácení akce zpět a obnovte ji nebo ji spusťte znovu.

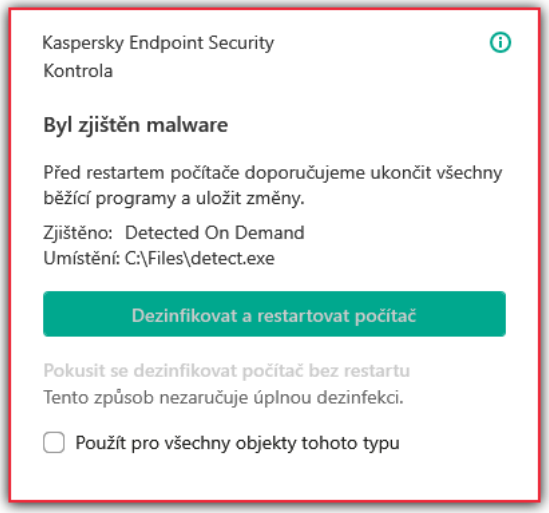
Práce s aktivními hrozbami

Aplikace Kaspersky Endpoint Security zaznamenává informace o souborech, které nebyly z nějakého důvody zpracovány. Tyto informace se zaznamenávají jako události na seznam aktivních hrozeb. Pro práci s aktivními hrozbami používá Kaspersky Endpoint Security technologii pokročilé dezinfekce. Pokročilá dezinfekce funguje jinak u pracovních stanic a serverů. Technologii pokročilé dezinfekce můžete nakonfigurovat v nastavení úlohy *Antivirová kontrola* a v nastavení aplikace.

Dezinfekce aktivních hrozeb na pracovních stanicích

Pro práci s aktivními hrozbami na pracovních stanicích povolte technologii pokročilé dezinfekce v nastavení aplikace. Dále nakonfigurujte činnost koncového uživatele v nastavení úlohy *Antivirová kontrola*. Ve vlastnostech úlohy je zaškrtávací políčko **Povolit okamžitou pokročilou dezinfekci**. Je-li tento příznak nastaven, aplikace Kaspersky Endpoint Security bude provádět dezinfekci bez upozornění uživatele. Po dokončení dezinfekce se počítač restartuje. Pokud příznak není nastaven, aplikace Kaspersky Endpoint Security zobrazí upozornění na aktivní hrozby (viz obrázek níže). Toto upozornění nemůžete zavřít bez zpracování souboru.

Pokročilá dezinfekce během úlohy antivirové kontroly v počítači je provedena, pouze pokud je ve vlastnostech zásad použitých na tento počítač povolena funkce Pokročilá dezinfekce.



Upozornění na aktivní hrozbu

Dezinfekce aktivních hrozeb na serverech

Pro práci s aktivními hrozbami na serverech musíte provést následující:

- povolit technologii Pokročilá dezinfekce v nastavení aplikace;
- povolit okamžitou pokročilou dezinfekci v nastavení úlohy *Antivirová kontrola* .

Je-li aplikace Kaspersky Endpoint Security nainstalována v počítači se systémem Windows pro servery, toto upozornění nezobrazí. Uživatel tak nemůže vybrat akci, která dezinfikuje aktivní hrozbu. Chcete-li dezinfikovat hrozbu, musíte v nastavení aplikace povolit technologii Pokročilá dezinfekce a ve vlastnostech *úlohy Antivirová kontrola* povolit okamžitou pokročilou dezinfekci. Poté musíte spustit úlohu *Antivirová kontrola*.

Zpracování aktivních hrozeb

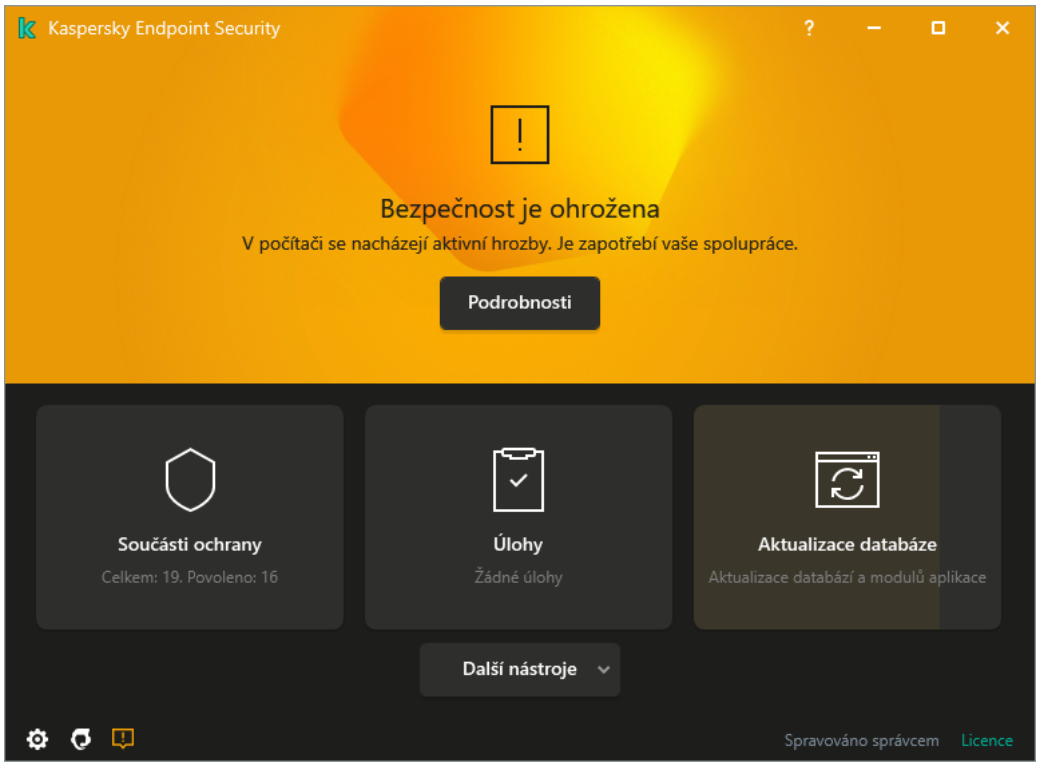
Infikovaný soubor je považován za *zpracovaný*, jestliže aplikace Kaspersky Endpoint Security provede během kontroly počítače na přítomnost virů a jiných hrozeb na daném souboru jednu z následujících akcí podle zadaného nastavení aplikace:

- Dezinfikovat.
- Odebrat.
- Odstranit, pokud se dezinfekce nezdaří.

Aplikace Kaspersky Endpoint Security přesune soubor na seznam aktivních hrozeb, jestliže z nějakého důvodu nedokáže během kontroly počítače na přítomnost virů a jiných hrozeb provést na daném souboru akci podle zadaného nastavení aplikace.

Tato situace může nastat v následujících případech:

- Kontrolovaný soubor není dostupný (například se nachází na síťové nebo vyměnitelné jednotce bez oprávnění pro zápis).
- V části **Akce při zjištění hrozby** je pro úlohy kontroly vybrána akce **Inform** a uživatel vyberte akci **Přeskočit**, když se mu zobrazí upozornění na infikovaný soubor.



Hlavní okno aplikace, když je detekována hrozba

Postup zpracování aktivních hrozeb:

1. V hlavním okně aplikace klikněte na tlačítko **Podrobnosti**.

   Otevře se seznam aktivních hrozeb.

2. Vyberte objekt, který chcete zpracovat.
3. Vyberte, jak chcete s hrozbou naložit:

- **Vyřešit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní.

- **Ignorovat**. Je-li vybrána tato možnost, aplikace Kaspersky Endpoint Security odstraní položku ze seznamu aktivních hrozeb. Až na seznamu nebudou zbývat žádné aktivní hrozby, stav počítače se změní na *OK*. V případě opětovného zjištění objektu přidá aplikace Kaspersky Endpoint Security do seznamu aktivních hrozeb novou položku.

- **Otevřít složku, ve které se nachází**. Je-li vybrána tato možnost, aplikace Kaspersky Endpoint Security ve správci souborů otevře složku, ve které se objekt nachází. Poté můžete objekt ručně odstranit nebo jej přesunout do složky, na niž se nevztahuje ochrana.

- **Další informace**. Je-li vybrána tato možnost, aplikace Kaspersky Endpoint Security otevře web encyklopedie virů společnosti Kaspersky.

Ochrana před souborovými hrozbami

Součásti Ochrana před souborovými hrozbami umožňuje zabránit infikování souborového systému počítače. Ve výchozím nastavení je součást Ochrana před souborovými hrozbami trvale uložena v paměti RAM počítače. Tato součást prohledává soubory na všech jednotkách počítače i na připojených jednotkách. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Součást prohledává soubory, k nimž přistoupil uživatel nebo aplikace. Pokud je zjištěn škodlivý soubor, aplikace Kaspersky Endpoint Security blokuje aktivitu tohoto souboru. Aplikace poté škodlivý soubor dezinfikuje nebo odstraní v závislosti na nastavení součásti Ochrana před souborovými hrozbami.

Když se pokusíte o přístup k souboru, jehož obsah je uložen v cloudu OneDrive, aplikace Kaspersky Endpoint Security stáhne a zkontroluje obsah tohoto souboru.

Povolení a zakázání součásti Ochrana před souborovými hrozbami

Ve výchozím nastavení je součást Ochrana před souborovými hrozbami povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. Pro ochranu před souborovými hrozbami může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto skupiny nastavení uložené v aplikaci se nazývají *úrovně zabezpečení*: **Vysoká**, **Doporučená**, **Nízká**. **Doporučená** nastavení úrovně zabezpečení jsou považována za optimální nastavení doporučená odborníky společnosti Kaspersky (viz tabulka níže). Můžete vybrat jednu z předvoleb úrovně zabezpečení nebo konfigurovat nastavení úrovně zabezpečení ručně. Pokud změníte nastavení úrovně zabezpečení, můžete se kdykoli vrátit zpět k doporučeným nastavením.

Postup povolení nebo zakázání součásti Ochrana před souborovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
3. Pomocí přepínače **Ochrana před souborovými hrozbami** můžete tuto součást povolit nebo zakázat.
4. Pokud jste součást povolili, v části **Úroveň zabezpečení** proveďte jednu z těchto akcí:
   - Chcete-li použít jednu z předvoleb úrovně zabezpečení, vyberte ji pomocí posuvníku:
     - **Vysoká**. Při výběru této úrovně zabezpečení souborů kontroluje součást Ochrana před souborovými hrozbami všechny otevírané, ukládané a spouštěné soubory tím nejpřísnějším způsobem. Součást Ochrana před souborovými hrozbami kontroluje všechny typy souborů na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače. Kontroluje rovněž archivy, balíčky instalační služby a vložené objekty OLE.
     - **Doporučená**. Tuto úroveň zabezpečení souborů doporučují specialisté společnosti Kaspersky. Součást Ochrana před souborovými hrozbami kontroluje pouze zadané formáty souborů, a to na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače a také vložené objekty OLE. Součást Ochrana před souborovými hrozbami nekontroluje archivy ani instalační balíčky. Hodnoty nastavení pro doporučenou úroveň zabezpečení jsou uvedeny v tabulce níže.

- **Nízká**. Nastavení této úrovně zabezpečení souborů zajišťuje maximální rychlost kontroly. Součást Ochrana před souborovými hrozbami kontroluje pouze soubory se zadanými příponami, a to na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače. Součást Ochrana před souborovými hrozbami nekontroluje složené soubory.

- Pokud chcete nakonfigurovat vlastní úroveň zabezpečení, klikněte na tlačítko **rozšířené nastavení** a definujte vlastní nastavení součásti.

  Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Obnovit doporučenou úroveň zabezpečení** v horní části okna.

5. Uložte změny.

Nastavení ochrany před souborovými hrozbami doporučená odborníky společnosti Kaspersky (doporučená úroveň zabezpečení)

Parametr	Hodnota	Popis
Typy souborů	**Soubory kontrolované podle formátu**	Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami.
Heuristická analýza	**Lehká kontrola**	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Kontrolovat pouze nové a změněné soubory	**Povoleno**	Kontroluje pouze nové soubory a soubory, které byly od posledního skenování změněny. To pomáhá zkrátit dobu skenování. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.
Technologie iSwift	**Povoleno**	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.
Technologie iChecker	**Povoleno**	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).
Kontrolovat soubory ve formátu aplikací Microsoft Office	**Povoleno**	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Režim kontroly	**Chytrý režim**	V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekt na základě analýzy akcí v tomto objektu provedených. Například při

		práci s dokumentem aplikace Microsoft Office provede aplikace Kaspersky Endpoint Security kontrolu souboru při jeho úvodním otevření a konečném zavření. Prozatímní operace, které přepisují soubor, jeho kontrolu nespouštějí.
Akce při zjištění hrozby	**Dezinfikovat. Jestliže to není možné, tak odstranit**	Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní.

Automatické pozastavení součásti Ochrana před souborovými hrozbami

Součást Ochrana před souborovými hrozbami můžete nastavit tak, aby se automaticky pozastavila v určenou dobu nebo při práci s určitými aplikacemi.

Součást Ochrana před souborovými hrozbami by měla být pozastavena pouze v krajním případě, když je v konfliktu s některými aplikacemi. Pokud během provozu součásti dojde ke konfliktu, doporučujeme vám kontaktovat technickou podporu společnosti Kaspersky. Odborníci podpory vám pomůžou nastavit součást Ochrana před souborovými hrozbami tak, aby mohla být v počítači používána současně s jinými aplikacemi.

Postup konfigurace automatického pozastavení součásti Ochrana před souborovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Pozastavení součásti Ochrana před souborovými hrozbami** klikněte na odkaz **Pozastavit součást Ochrana před souborovými hrozbami**.
5. V okně, které se otevře, nakonfigurujte nastavení pro pozastavení součásti Ochrana před souborovými hrozbami:
   a. Nakonfigurujte plán automatického pozastavování součásti Ochrana před souborovými hrozbami.
   b. Vytvořte seznam aplikací, jejichž provoz by měl způsobit pozastavení činnosti součásti Ochrana před souborovými hrozbami.
6. Uložte změny.

Změna akce, kterou součást Ochrana před souborovými hrozbami provede s infikovanými soubory

Ve výchozím nastavení se součást Ochrana před souborovými hrozbami automaticky pokusí všechny zjištěné infikované soubory automaticky dezinfikovat. Jestliže se soubory nepodaří dezinfikovat, součást Ochrana před souborovými hrozbami je odstraní.

Postup změny akce, kterou součást Ochrana před souborovými hrozbami provede s infikovanými soubory:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. V části **Akce při zjištění hrozby** vyberte požadovanou možnost:
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní.
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.
   - **Blokovat**. Pokud je vybrána tato možnost, bude součást Ochrana před souborovými hrozbami všechny infikované soubory automaticky blokovat, aniž by se je pokusila dezinfikovat.

   Před pokusem o dezinfekci nebo odstranění infikovaného souboru vytvoří aplikace Kaspersky Endpoint Security záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.
4. Uložte změny.

Vytvoření rozsahu ochrany součásti Ochrana před souborovými hrozbami

Rozsah ochrany označuje objekty, které součást při povolení kontroluje. Rozsahy ochrany pomocí různých součástí mají různé vlastnosti. Umístění a typ souborů ke kontrole jsou vlastnosti rozsahu ochrany v součásti Ochrana před souborovými hrozbami. Ve výchozím nastavení součást Ochrana před souborovými hrozbami kontroluje pouze potenciálně infikovatelné soubory, které jsou spouštěny z pevných disků, vyměnitelných disků a síťových disků.

Při volbě typů souborů ke kontrole mějte na paměti následující informace:

1. Existuje nízká pravděpodobnost zavedení škodlivého kódu do souborů určitých formátů a jeho následné aktivace (například formát TXT). Existují však některé formáty souborů, které obsahují spustitelný kód (např. .exe, .dll nebo .doc). Spustitelný kód mohou také obsahovat soubory formátů, které nejsou pro tento účel určeny (například formát DOC). U těchto souborů je riziko narušení pomocí škodlivého kódu a jeho aktivace velké.
2. Narušitel může odeslat virus nebo jinou škodlivou aplikaci do počítače ve formě spustitelného souboru, který je přejmenovaný a má příponu .txt. Pokud vyberete kontrolu souborů podle přípony, aplikace při kontrole takový soubor přeskočí. Pokud je vybrána kontrola souborů podle formátu, aplikace Kaspersky Endpoint Security analyzuje záhlaví souboru bez ohledu na příponu. Pokud tato analýza odhalí, že soubor má formát spustitelného souboru (například EXE), aplikace jej zkontroluje.

Postup vytvoření rozsahu ochrany:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V části **Typy souborů** zadejte typy souborů, které má součást Ochrana před souborovými hrozbami kontrolovat:

   - **Všechny soubory**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje všechny soubory bez výjimky (všechny formáty a přípony).

   - **Soubory kontrolované podle formátu**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami.

   - **Soubory kontrolované podle přípony**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.

5. Klikněte na odkaz **Upravit rozsah ochrany**.

6. V okně, které se otevře, vyberte objekty, které chcete přidat do rozsahu ochrany nebo z něj vyloučit.

   Objekty, které jsou ve výchozím rozsahu ochrany, nelze odebírat ani upravovat.

7. Pokud chcete do rozsahu ochrany přidat nový objekt:

   a. Klikněte na tlačítko **Přidat**.

      Otevře se strom složek.

   b. Vyberte objekt a klikněte na tlačítko **Vybrat**.

   Objekt můžete z kontroly vyloučit, aniž byste jej odstranili ze seznamu objektů v rozsahu kontroly. Chcete-li tak učinit, zrušte zaškrtnutí políčka vedle objektu.

8. Uložte změny.

Použití metod kontroly

Aplikace Kaspersky Endpoint Security používá metodu kontroly zvanou strojové učení a analýza signatur. Během analýzy podle databází spáruje aplikace Kaspersky Endpoint Security zjištěné objekty se záznamy v databázi. Na základě doporučení odborníků společnosti Kaspersky je metoda strojového učení a analýzy signatur vždy povolena.

Chcete-li zvýšit účinnost ochrany, můžete použít heuristickou analýzu. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.

Postup konfigurace použití heuristické analýzy při provozu součásti Ochrana před souborovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. Pokud chcete, aby aplikace k ochraně před souborovými hrozbami používala heuristickou analýzu, v bloku **Metody kontroly** zaškrtněte políčko **Heuristická analýza**. Poté pomocí posuvníku nastavte úroveň heuristické analýzy: **Lehká kontrola**, **Střední kontrola** nebo **Hloubková kontrola**.

5. Uložte změny.

Použití technologií kontroly při provozu součásti Ochrana před souborovými hrozbami

Postup konfigurace použití technologií kontroly při provozu součásti Ochrana před souborovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V části **Technologie kontroly** zaškrtněte políčka vedle názvů technologií, které chcete použít pro ochranu před souborovými hrozbami:

   - **Technologie iSwift**. Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.

   - **Technologie iChecker**. Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).

5. Uložte změny.

Optimalizace kontroly souborů

Zkrácením doby kontroly a zvýšením provozní rychlosti aplikace Kaspersky Endpoint Security můžete optimalizovat kontrolu souborů prováděnou součástí Ochrana před souborovými hrozbami. Toho lze dosáhnout tak, že budou kontrolovány jen nové soubory a soubory, které byly od předchozí kontroly změněny. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.

Můžete také povolit použití technologií iChecker a iSwift, které optimalizují rychlost kontroly souborů tím, že jsou vyloučeny soubory, které nebyly od poslední kontroly změněny.

Postup optimalizace kontroly souborů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V části **Optimalizace kontroly** zaškrtněte políčko **Kontrolovat pouze nové a změněné soubory**.
5. Uložte změny.

Kontrola složených souborů

Častou technikou ukrývání virů a jiného malwaru je jejich implantace do složených souborů, jakými jsou archivy či databáze. Aby bylo možné zjistit viry a jiný malware skrytý tímto způsobem, složený soubor musí být rozbalen, což může zpomalit kontrolu. Typy kontrolovaných složených souborů můžete omezit a tím kontrolu urychlit.

Způsob použitý ke zpracování infikovaného složeného souboru (dezinfekce nebo odstranění) je závislý na typu souboru.

Součást Ochrana před souborovými hrozbami dezinfikuje složené soubory ve formátech RAR, ARJ, ZIP, CAB a LHA a odstraní soubory ve všech jiných formátech (kromě databází pošty).

Postup konfigurace kontroly složených souborů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V části **Kontrola složených souborů** zadejte typy složených souborů, které chcete kontrolovat: archivy, instalační balíčky nebo soubory ve formátech sady Office.
5. Pokud je zakázána kontrola pouze nových a upravených souborů, nakonfigurujte nastavení pro kontrolu každého typu složeného souboru: kontrolovat všechny soubory tohoto typu nebo pouze nové soubory.

   Pokud je povolena kontrola pouze nových a upravených souborů, Kaspersky Endpoint Security kontroluje pouze nové a upravené soubory všech typů složených souborů.
6. Nakonfigurujte rozšířené nastavení pro kontrolu složených souborů.

   - **Nerozbalovat velké složené soubory**.

     Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu.

     Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security zkontroluje složené soubory všech velikostí.

Aplikace Kaspersky Endpoint Security kontroluje velké soubory extrahované z archivů bez ohledu na to, zda je či není zaškrtnuto políčko **Nerozbalovat velké složené soubory**.

- **Rozbalit složené soubory na pozadí**.

  Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům, které jsou větší než zadaná hodnota, před kontrolou těchto souborů. V tomto případě aplikace Kaspersky Endpoint Security rozbalí a zkontroluje složené soubory na pozadí.

  Aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům, které jsou menší než tato hodnota, až po rozbalení a kontrole těchto souborů.

  Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům pouze po rozbalení a kontrole souborů jakékoli velikosti.

7. Uložte změny.

Změna režimu kontroly

Režim kontroly označuje podmínku, která spustí kontrolu souboru pomocí součásti Ochrana před souborovými hrozbami. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje soubory v chytrém režimu. V tomto režimu kontroly souborů se součást Ochrana před souborovými hrozbami rozhodne, zda soubory kontrolovat či nikoli: po provedení analýzy operací prováděných se souborem ze strany uživatele, ze strany aplikace jménem uživatele (v rámci účtu, který byl použit k přihlášení, nebo v rámci jiného uživatelského účtu) nebo ze strany operačního systému. Například při práci s dokumentem aplikace Microsoft Office Word provede aplikace Kaspersky Endpoint Security kontrolu souboru při jeho úvodním otevření a konečném zavření. Prozatímní operace, které přepisují soubor, jeho kontrolu nespouštějí.

Postup změny režimu kontroly souborů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana → Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V části **Režim kontroly** vyberte požadovaný režim:

   - **Chytrý režim**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekt na základě analýzy akcí v tomto objektu provedených. Například při práci s dokumentem aplikace Microsoft Office provede aplikace Kaspersky Endpoint Security kontrolu souboru při jeho úvodním otevření a konečném zavření. Prozatímní operace, které přepisují soubor, jeho kontrolu nespouštějí.

   - **Při přístupu a změnách**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty při každém pokusu o jejich otevření nebo změnu.

   - **Při přístupu**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich otevření.

   - **Při spuštění**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich spuštění.

5. Uložte změny.

Ochrana před webovými hrozbami

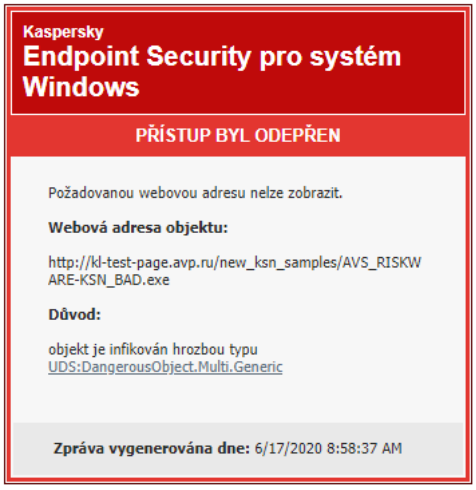
Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Ochrana před webovými hrozbami zabraňuje stahování škodlivých souborů z internetu a blokuje škodlivé a phishingové weby. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Aplikace Kaspersky Endpoint Security kontroluje pouze provoz HTTP, HTTPS a FTP. Aplikace Kaspersky Endpoint Security kontroluje adresy URL a IP adresy. Můžete určit porty, které bude Kaspersky Endpoint Security sledovat, nebo vybrat všechny porty.

Pro sledování provozu HTTPS je třeba povolit kontroly šifrovaných připojení.

Když se uživatel pokusí otevřít škodlivý nebo phishingový web, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).



Zpráva o odepření přístupu na web

Povolení a zakázání součásti Ochrana před webovými hrozbami

Ve výchozím nastavení je součást Ochrana před webovými hrozbami povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. Pro ochranu před webovými hrozbami může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto skupiny nastavení uložené v aplikaci se nazývají *úrovně zabezpečení*: **Vysoká**, **Doporučená**, **Nízká**. **Doporučená** nastavení úrovně zabezpečení webového provozu jsou považována za optimální nastavení doporučená odborníky společnosti Kaspersky. Můžete vybrat jednu z předinstalovaných úrovní zabezpečení webového provozu přenášeného mezi počítačem a externí lokalitou přes protokoly HTTP a FTP, případně můžete pro webový provoz nastavit vlastní úroveň zabezpečení. Pokud nastavení úrovně zabezpečení webového provozu změníte, můžete se kdykoli vrátit k doporučeným nastavením úrovně zabezpečení.

Postup povolení nebo zakázání součásti Ochrana před webovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.

3. Pomocí přepínače **Ochrana před webovými hrozbami** můžete tuto součást povolit nebo zakázat.

4. Pokud jste součást povolili, v části **Úroveň zabezpečení** proveďte jednu z těchto akcí:

   - Chcete-li použít jednu z předvoleb úrovně zabezpečení, vyberte ji pomocí posuvníku:

     - **Vysoká**. Úroveň zabezpečení, při které součást Ochrana před webovými hrozbami provádí maximální kontrolu webového provozu uskutečněného prostřednictvím protokolů HTTP a FTP směrem k počítači. Součást Ochrana před webovými hrozbami bude podrobně kontrolovat všechny objekty webového provozu pomocí všech databází aplikace a provádět nejpodrobnější možnou heuristickou analýzu.

     - **Doporučená**. Úroveň zabezpečení e-mailů, která poskytuje optimální rovnováhu mezi výkonem aplikace Kaspersky Endpoint Security a zabezpečením webového provozu. Součást Ochrana před webovými hrozbami bude provádět heuristickou analýzu na úrovni **Střední kontrola**. Tuto úroveň zabezpečení webového provozu doporučují specialisté společnosti Kaspersky. Hodnoty nastavení pro doporučenou úroveň zabezpečení jsou uvedeny v tabulce níže.

     - **Nízká**. Nastavení této úrovně zabezpečení webového provozu zajišťuje nejrychlejší kontrolu webového provozu. Součást Ochrana před webovými hrozbami bude provádět heuristickou analýzu na úrovni **Lehká kontrola**.

   - Pokud chcete nakonfigurovat vlastní úroveň zabezpečení, klikněte na tlačítko **rozšířené nastavení** a definujte vlastní nastavení součásti.

     Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Obnovit doporučenou úroveň zabezpečení** v horní části okna.

5. Uložte změny.

Nastavení ochrany před webovými hrozbami doporučená odborníky společnosti Kaspersky (doporučená úroveň zabezpečení)

Parametr	Hodnota	Popis
Zkontrolovat, zda jsou odkazy uvedeny v databázi škodlivých odkazů	**Povoleno**	Kontrola odkazů za účelem zjištění, zda jsou zahrnuty do databáze škodlivých webových adres, umožňuje sledovat weby, které byly na seznamu zakázaných webů. Databáze škodlivých webových adres je spravována společností Kaspersky, je zahrnuta v instalačním balíčku aplikace a aktualizována během aktualizací databáze aplikace Kaspersky Endpoint Security.
Porovnat adresu URL s databází phishingových adres URL	**Povoleno**	Databáze phishingových webových adres zahrnuje webové adresy aktuálně známých webových stránek, které se používají ke spuštění phishingových útoků. Společnost Kaspersky doplňuje tuto databázi phishingových odkazů o adresy získané od mezinárodní organizace známé jako Anti-Phishing Working Group. Databáze phishingových webových adres je zahrnuta v instalačním balíčku aplikace a doplňována aktualizacemi databáze aplikace Kaspersky Endpoint Security.
Použít heuristickou analýzu (Ochrana před webovými hrozbami)	**Střední kontrola**	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru.

		Když se u webového provozu kontroluje přítomnost virů a dalších aplikací, které představují hrozbu, provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Použít heuristickou analýzu (Anti-Phishing)	**Povoleno**	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru.
Akce při zjištění hrozby	**Blokovat stahování**	Pokud je vybrána tato možnost a ve webovém provozu je zjištěn infikovaný objekt, součást Ochrana před webovými hrozbami zablokuje přístup k tomuto objektu a v prohlížeči zobrazí zprávu.

Změna akce, která se má provést se škodlivými objekty webového provozu

Ve výchozím nastavení součást Ochrana před webovými hrozbami při zjištění infikovaného objektu ve webovém provozu zablokuje přístup k tomuto objektu a zobrazí oznámení o příslušné akci.

Postup změny akce, která bude provedena se škodlivými objekty webového provozu:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
3. V části **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty webového provozu:
   - **Blokovat stahování**. Pokud je vybrána tato možnost a ve webovém provozu je zjištěn infikovaný objekt, součást Ochrana před webovými hrozbami zablokuje přístup k tomuto objektu a v prohlížeči zobrazí zprávu.
   - **Informovat**. Pokud je vybrána tato možnost a ve webovém provozu je zjištěn infikovaný objekt, aplikace Kaspersky Endpoint Security umožní tento objekt stáhnout do počítače, ale přidá informace o infikovaném objektu do seznamu aktivních hrozeb.
4. Uložte změny.

Porovnání adres URL s databázemi phishingových a škodlivých webových adres

Kontrola, zda odkazy nejsou na seznamu phishingových webových adres, umožňuje zabránit *phishingovým útokům*. Phishingový útok může být skrytý například v e-mailové zprávě, která se jeví jako zpráva zřejmě od vaší banky s odkazem na oficiální web banky. Kliknutím na odkaz přejdete na přesnou kopii webových stránek banky a v prohlížeči může být dokonce uvedena její skutečná webová adresa, i když jste na falešných stránkách. Od tohoto okamžiku jsou všechny vaše akce provedené na webu sledovány a mohou být použity k odcizení vašich peněz.

Odkazy na phishingové webové stránky lze přijmout nejen v e-mailu, ale také z jiných zdrojů, jako jsou například zprávy ICQ, proto součást Ochrana před webovými hrozbami sleduje pokusy o přístup k phishingovým webovým stránkám na úrovni kontroly webového provozu a přístup na takové webové stránky blokuje. Seznamy phishingových adres URL jsou součástí distribučního balíčku aplikace Kaspersky Endpoint Security.

Postup konfigurace kontroly odkazů prováděných součástí Ochrana před webovými hrozbami za použití databází phishingových a škodlivých webových adres:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Postupujte následovně:
   - Pokud chcete, aby součást Ochrana před webovými hrozbami kontrolovala odkazy za použití databází škodlivých webových adres, v části **Metody kontroly** zaškrtněte políčko **Porovnat adresu URL s databází škodlivých adres URL**. Kontrola odkazů za účelem zjištění, zda jsou zahrnuty do databáze škodlivých webových adres, umožňuje sledovat weby, které byly na seznamu zakázaných webů. Databáze škodlivých webových adres je spravována společností Kaspersky, je zahrnuta v instalačním balíčku aplikace a aktualizována během aktualizací databáze aplikace Kaspersky Endpoint Security.

     Kaspersky Endpoint kontroluje všechny odkazy a určuje, zda jsou uvedeny v databázích škodlivých webových adres. Na funkčnost kontroly odkazů nemá vliv nastavení kontroly bezpečného připojení aplikace. Jinými slovy, pokud jsou zakázány kontroly šifrovaného připojení, kontroluje aplikace Kaspersky Endpoint Security v databázích škodlivých webových adres, i když je síťový provoz přenášen přes šifrované připojení.

   - Pokud chcete, aby součást Ochrana před webovými hrozbami kontrolovala odkazy v databázích phishingových webových adres, zaškrtněte v bloku **Anti-Phishing** políčko **Porovnat adresu URL s databází phishingových adres URL**. Databáze phishingových webových adres zahrnuje webové adresy aktuálně známých webových stránek, které se používají ke spuštění phishingových útoků. Společnost Kaspersky doplňuje tuto databázi phishingových odkazů o adresy získané od mezinárodní organizace známé jako Anti-Phishing Working Group. Databáze phishingových webových adres je zahrnuta v instalačním balíčku aplikace a doplňována aktualizacemi databáze aplikace Kaspersky Endpoint Security.

     Odkazy lze kontrolovat také za použití databází reputace ve službě Kaspersky Security Network.

5. Uložte změny.

Použití heuristické analýzy při provozu součásti Ochrana před webovými hrozbami

Chcete-li zvýšit účinnost ochrany, můžete použít heuristickou analýzu. Aplikace Kaspersky Endpoint Security během heuristické analýzy analyzuje činnost aplikací v operačním systému. Heuristická analýza umožňuje zjistit hrozby, o nichž aktuálně nejsou v databázích aplikace Kaspersky Endpoint Security žádné záznamy.

Konfigurace použití heuristické analýzy:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Pokud chcete, aby aplikace při kontrole webového provozu na přítomnost virů a dalšího malwaru používala heuristickou analýzu, v bloku **Metody kontroly** zaškrtněte políčko **Použít heuristickou analýzu**. Poté pomocí posuvníku nastavte úroveň heuristické analýzy: **Lehká kontrola**, **Střední kontrola** nebo **Hloubková kontrola**.
5. Pokud chcete, aby aplikace při kontrole webového provozu na přítomnost phishingových odkazů používala heuristickou analýzu, v bloku **Anti-Phishing** zaškrtněte políčko **Použít heuristickou analýzu**.
6. Uložte změny.

Vytvoření seznamu důvěryhodných webových adres

Můžete vytvořit seznam adres URL s obsahem, kterému důvěřujete. Součást Ochrana před webovými hrozbami neanalyzuje informace z důvěryhodných webových adres, aby na nich zkontrolovala viry a další hrozby. Tato možnost může být užitečná, když součást Ochrana před webovými hrozbami například zasáhne do stahování souboru ze známých webových stránek.

Adresa URL může být adresou webu nebo určité webové stránky.

Vytvoření seznamu důvěryhodných webových adres:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Zaškrtněte políčko **Nekontrolovat webový provoz z důvěryhodných webových adres**.

   Pokud je toto políčko zaškrtnuto, nebude součást Ochrana před webovými hrozbami kontrolovat obsah webových stránek nebo webů, jejichž adresy jsou uvedeny v seznamu důvěryhodných webových adres. Konkrétní adresu i masku adresy webové stránky nebo webu lze přidat do seznamu důvěryhodných webových adres.
5. Vytvořte seznam adres URL / webových stránek s důvěryhodným obsahem.
6. Uložte změny.

Export a import seznamu důvěryhodných webových adres

Seznam důvěryhodných webových adres můžete exportovat do souboru XML. Poté můžete soubor upravit, například přidat velké množství webových adres stejného typu. Můžete také použít funkci exportu/importu k zálohování seznamu důvěryhodných webových adres nebo k migraci seznamu na jiný server.

[Jak exportovat a importovat seznam důvěryhodných webových adres v konzole pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
6. Klikněte na tlačítko **Nastavení**.
7. V okně, které se otevře, vyberte kartu **Důvěryhodné webové adresy**.
8. Postup exportu seznamu důvěryhodných webových adres:
   a. Vyberte důvěryhodné webové adresy, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste nevybrali žádnou důvěryhodnou webovou adresu, aplikace Kaspersky Endpoint Security exportuje všechny webové adresy.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam důvěryhodných webových adres, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam důvěryhodných adres do souboru XML.
9. Postup importu seznamu důvěryhodných adres:
   a. Klikněte na odkaz **Importovat**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam důvěryhodných adres.
   b. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam důvěryhodných adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.
10. Uložte změny.

[Jak exportovat a importovat seznam důvěryhodných webových adres ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam důvěryhodných webových adres.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
5. Postup exportu seznamu výjimek v bloku **Důvěryhodné webové adresy**:
   a. Vyberte důvěryhodné webové adresy, které chcete exportovat.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam důvěryhodných webových adres, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam důvěryhodných adres do souboru XML.
6. Postup importu seznamu výjimek v bloku **Důvěryhodné webové adresy**:
   a. Klikněte na odkaz **Importovat**.

      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam důvěryhodných adres.
   b. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam důvěryhodných adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.
7. Uložte změny.

Ochrana před hrozbami v poště

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Ochrana před hrozbami v poště v přílohách kontroluje, zda příchozí a odchozí e-maily obsahují viry nebo jiné hrozby. Tato součást také kontroluje zprávy, zda neobsahují škodlivé a phishingové odkazy. Ve výchozím nastavení je součást Ochrana před hrozbami v poště trvale uložena v paměti RAM počítače a prohledává všechny zprávy přijaté nebo odeslané pomocí protokolů POP3, SMTP, IMAP nebo NNTP nebo poštovního klienta Microsoft Office Outlook (MAPI). Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Součást Ochrana před hrozbami v poště nekontroluje zprávy, pokud je poštovní klient otevřen v prohlížeči.

Jestliže je v příloze detekován škodlivý soubor, Kaspersky Endpoint Security přejmenuje předmět zprávy: `[Zpráva je infikována] <předmět zprávy>` nebo `[Infikovaný objekt odstraněn] <předmět zprávy>`.

Tato součást komunikuje s e-mailovými klienty nainstalovanými v počítači. U poštovního klienta aplikace Microsoft Office Outlook je k dispozici rozšíření s dalšími parametry. Rozšíření Ochrana před hrozbami v poště se vloží do e-mailového klienta Microsoft Office Outlook během instalace aplikace Kaspersky Endpoint Security.

Povolení a zakázání součásti Ochrana před hrozbami v poště

Ve výchozím nastavení je součást Ochrana před hrozbami v poště povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. Pro ochranu před hrozbami v poště může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto skupiny nastavení uložené v aplikaci se nazývají *úrovně zabezpečení*: **Vysoká**, **Doporučená**, **Nízká**. **Doporučená** nastavení úrovně zabezpečení pošty jsou považována za optimální nastavení doporučená odborníky společnosti Kaspersky. Můžete vybrat jednu z předvoleb úrovně zabezpečení e-mailových zpráv nebo nakonfigurovat vlastní. Pokud jste nastavení úrovně zabezpečení e-mailových zpráv změnili, můžete se kdykoli vrátit k doporučeným nastavením.

Postup povolení nebo zakázání součásti Ochrana před hrozbami v poště:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
3. Pomocí přepínače **Ochrana před hrozbami v poště** můžete tuto součást povolit nebo zakázat.
4. Pokud jste součást povolili, v části **Úroveň zabezpečení** proveďte jednu z těchto akcí:
   - Chcete-li použít jednu z předvoleb úrovně zabezpečení, vyberte ji pomocí posuvníku:
     - **Vysoká**. Je-li vybrána tato úroveň zabezpečení e-mailů, součást Ochrana před hrozbami v poště kontroluje e-mailové zprávy nejdůkladněji. Součást Ochrana před hrozbami v poště kontroluje příchozí a odchozí e-mailové zprávy a provede podrobnou heuristickou analýzu. Úroveň zabezpečení pošty **Vysoká** se doporučuje pro vysoce riziková prostředí. Příkladem takového prostředí je připojení k bezplatné e-mailové službě z domácí sítě, která není hlídaná centralizovanou e-mailovou ochranou.
     - **Doporučená**. Úroveň zabezpečení e-mailů, která poskytuje optimální rovnováhu mezi výkonem aplikace Kaspersky Endpoint Security a zabezpečením e-mailů. Součást Ochrana před hrozbami v poště kontroluje příchozí a odchozí e-mailové zprávy a provede heuristickou analýzu střední úrovně. Tato úroveň zabezpečení e-mailového provozu je doporučena odborníky společnosti Kaspersky. Hodnoty nastavení pro doporučenou úroveň zabezpečení jsou uvedeny v tabulce níže.
     - **Nízká**. Při výběru této úrovně zabezpečení e-mailů bude součást Ochrana před hrozbami v poště kontrolovat pouze příchozí e-mailové zprávy a provádět zběžnou heuristickou analýzu. Nebude kontrolovat archivy, které jsou připojeny k e-mailovým zprávám. Na této úrovni zabezpečení e-mailů kontroluje součást Ochrana před hrozbami v poště e-mailové zprávy maximální rychlostí a využívá minimum prostředků operačního systému. **Nízká** úroveň zabezpečení e-mailů je doporučena pro dobře chráněná prostředí. Příkladem takovéhoto prostředí může být podniková síť LAN s centralizovaným zabezpečením pošty.

- Pokud chcete nakonfigurovat vlastní úroveň zabezpečení, klikněte na tlačítko **rozšířené nastavení** a definujte vlastní nastavení součásti.

  Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Obnovit doporučenou úroveň zabezpečení** v horní části okna.

5. Uložte změny.

Nastavení ochrany před hrozbami v poště doporučená odborníky společnosti Kaspersky (doporučená úroveň zabezpečení)

Parametr	Hodnota	Popis
Rozsah ochrany	**Příchozí a odchozí zprávy**	*Rozsah ochrany* zahrnuje objekty, které součást při spuštění kontroluje: **Příchozí a odchozí zprávy** nebo **Pouze příchozí zprávy**. Chcete-li chránit své počítače, musíte kontrolovat pouze příchozí zprávy. Abyste zabránili odesílání infikovaných souborů v archivech, můžete zapnout kontrolu odchozích zpráv. Kontrolu odchozích zpráv můžete také zapnout, pokud chcete zabránit odesílání souborů v určitých formátech, například zvukových a obrazových souborů.
Připojovat rozšíření pro Microsoft Outlook	**Povoleno**	Pokud je políčko zaškrtnuto, kontrola e-mailových zpráv přenášených přes protokoly POP3, SMTP, NNTP a IMAP je povolena na straně rozšíření integrovaného do aplikace Microsoft Outlook. Pokud je e-mail kontrolován pomocí rozšíření pro aplikaci Microsoft Outlook, doporučujeme použít režim serveru Exchange s mezipamětí. Podrobnější informace o režimu serveru Exchange s mezipamětí a o doporučeních k jeho použití najdete ve znalostní bázi Microsoft Knowledge Base.
Kontrolovat připojené archivy	**Povoleno**	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
Kontrola přiložených formátů sady Office	**Povoleno**	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Filtr příloh	**Přejmenovat přílohy vybraného typu**	Pokud je tato možnost vybrána, nahradí součást Ochrana před hrozbami v poště poslední znak v připojených souborech zadaných typů symbolem podtržítka (například priloha.doc_). Uživatel tedy musí soubor přejmenovat, aby jej mohl otevřít.
Heuristická analýza	**Střední kontrola**	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Akce při zjištění hrozby	**Dezinfikovat. Jestliže to není možné, tak odstranit**	Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, Kaspersky Endpoint Security tento objekt odstraní. Aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci: `[Byl odstraněn infikovaný objekt] <předmět zprávy>`.

Změna akce, která bude provedena s infikovanými e-mailovými zprávami

Ve výchozím nastavení se součást Ochrana před hrozbami v poště pokusí všechny zjištěné infikované e-mailové zprávy automaticky dezinfikovat. Jestliže se infikované e-mailové zprávy nepodaří dezinfikovat, součást Ochrana před hrozbami v poště je odstraní.

Postup změny akce, která bude provedena s infikovanými e-mailovými zprávami:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
3. V části **Akce při zjištění hrozby** vyberte akci, kterou aplikace Kaspersky Endpoint Security provede v případě zjištění infikované zprávy:
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, Kaspersky Endpoint Security tento objekt odstraní. Aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci: `[Byl odstraněn infikovaný objekt] <předmět zprávy>`.
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace Kaspersky Endpoint Security k předmětu zprávy upozornění: `[Infikovaná zpráva]` <předmět zprávy>. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace Kaspersky Endpoint Security zablokuje přenos zprávy a poštovní klient zobrazí chybu.
   - **Blokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace Kaspersky Endpoint Security k předmětu zprávy upozornění: `[Infikovaná zpráva] <předmět zprávy>`. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace Kaspersky Endpoint Security zablokuje přenos zprávy a poštovní klient zobrazí chybu.
4. Uložte změny.

Vytvoření rozsahu ochrany součásti Ochrana před hrozbami v poště

Rozsah ochrany označuje objekty, které součást během svého provozu kontroluje. Rozsahy ochrany pomocí různých součástí mají různé vlastnosti. Vlastnosti rozsahu ochrany součásti Ochrana před hrozbami v poště zahrnují nastavení integrace součásti Ochrana před hrozbami v poště do e-mailových klientů a typy e-mailových zpráv a e-mailových protokolů, jejichž provoz je kontrolován součástí Ochrana před hrozbami v poště. Ve výchozím nastavení kontroluje aplikace Kaspersky Endpoint Security příchozí i odchozí e-mailové zprávy a provoz protokolů POP3, SMTP, NNTP a IMAP a je integrována do e-mailového klienta Microsoft Office Outlook.

Postup vytvoření rozsahu ochrany součásti Ochrana před hrozbami v poště:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.

3. Klikněte na tlačítko **Rozšířené nastavení**.

4. V bloku **Rozsah ochrany** vyberte zprávy ke kontrole:

   - **Příchozí a odchozí zprávy**.
   - **Pouze příchozí zprávy**.

   Chcete-li chránit své počítače, musíte kontrolovat pouze příchozí zprávy. Abyste zabránili odesílání infikovaných souborů v archivech, můžete zapnout kontrolu odchozích zpráv. Kontrolu odchozích zpráv můžete také zapnout, pokud chcete zabránit odesílání souborů v určitých formátech, například zvukových a obrazových souborů.

   Pokud se rozhodnete kontrolovat pouze příchozí zprávy, doporučujeme vám provést jednorázovou kontrolu všech odchozích zpráv, protože existuje možnost, že váš počítač obsahuje e-mailové červy, kteří se rozšiřují prostřednictvím e-mailů. Můžete tak předejít problémům vzešlých z nepozorovaného hromadného rozesílání infikovaných e-mailů z vašeho počítače.

5. V části **Připojení** proveďte následující:

   - Chcete-li, aby součást Ochrana před hrozbami v poště kontrolovala zprávy, které jsou přenášeny prostřednictvím protokolů POP3, SMTP, NNTP a IMAP, než budou doručeny do počítače uživatele, zaškrtněte políčko **Kontrolovat přenosy POP3/SMTP/NNTP/IMAP**.

     Pokud nechcete, aby součást Ochrana před hrozbami v poště kontrolovala zprávy, které jsou přenášeny prostřednictvím protokolů POP3, SMTP, NNTP a IMAP, než budou doručeny do vašeho počítače, zaškrtnutí políčka **Kontrolovat přenosy POP3/SMTP/NNTP/IMAP** zrušte. V tomto případě budou zprávy kontrolovány rozšířením Ochrana před hrozbami v poště integrovaným v e-mailovém klientovi Microsoft Office Outlook po doručení do uživatelského počítače, pokud je zaškrtnuto políčko **Připojovat rozšíření pro Microsoft Outlook**.

     Používáte-li jiného e-mailového klienta než Microsoft Office Outlook, součást Ochrana před hrozbami v poště nebude zprávy přenášené prostřednictvím protokolů POP3, SMTP, NNTP a IMAP kontrolovat, pokud není zaškrtnuto políčko **Kontrolovat přenosy POP3/SMTP/NNTP/IMAP**.

   - Chcete-li povolit přístup k nastavení součásti Ochrana před hrozbami v poště z aplikace Microsoft Office Outlook a povolit kontrolu zpráv přenášených prostřednictvím protokolů POP3, SMTP, NNTP, IMAP a MAPI po jejich doručení do počítače za použití rozšíření integrovaného do aplikace Microsoft Office Outlook, zaškrtněte políčko **Připojovat rozšíření pro Microsoft Outlook**.

     Chcete-li blokovat přístup k nastavení součásti Ochrana před hrozbami v poště z aplikace Microsoft Office Outlook a zakázat kontrolu zpráv přenášených prostřednictvím protokolů POP3, SMTP, NNTP, IMAP a MAPI po jejich doručení do počítače za použití rozšíření integrovaného do aplikace Microsoft Office Outlook, zrušte zaškrtnutí políčka **Připojovat rozšíření pro Microsoft Outlook**.

     Rozšíření Ochrana před hrozbami v poště se vloží do e-mailového klienta Microsoft Office Outlook během instalace aplikace Kaspersky Endpoint Security.

6. Uložte změny.

Kontrola složených souborů přiložených k e-mailovým zprávám

Můžete povolit nebo zakázat kontrolu příloh zpráv, omezit maximální velikost kontrolovaných příloh zpráv a omezit maximální dobu trvání kontroly příloh zpráv.

Postup konfigurace kontroly složených souborů přiložených k e-mailovým zprávám:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V části **Kontrola složených souborů** nakonfigurujte nastavení kontroly:
   - **Kontrolovat přiložené soubory ve formátu aplikací Microsoft Office**. Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
   - **Kontrolovat připojené archivy**. Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.

     Pokud aplikace Kaspersky Endpoint Security během kontroly zjistí v textu zprávy heslo k archivu, bude toto heslo použito ke kontrole obsahu archivu na škodlivé aplikace. V tomto případě se heslo neukládá. Archiv je během kontroly rozbalen. Pokud během rozbalování dojde k chybě aplikace, můžete ručně odstranit rozbalené soubory, které jsou uloženy na následující cestě: %systemroot%\temp. Soubory mají předponu PR.

   - **Nekontrolovat archivy větší než N MB**. Pokud je toto políčko zaškrtnuto, vyloučí součást Ochrana před hrozbami v poště z kontroly archivy připojené k e-mailovým zprávám, jejichž velikost překračuje zadanou hodnotu. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude součást Ochrana před hrozbami v poště kontrolovat archivy připojené k e-mailovým zprávám, a to bez ohledu na jejich velikost.
   - **Omezit dobu kontroly archivu na N sekund**. Je-li políčko zaškrtnuto, doba přidělená kontrole archivů připojených k e-mailovým zprávám je omezena na zadanou dobu.
5. Uložte změny.

Filtrování příloh e-mailových zpráv

Funkce filtrování příloh se nepoužije na odchozí e-mailové zprávy.

Škodlivé aplikace mohou být rozšiřovány v podobě příloh v e-mailových zprávách. Je možné nakonfigurovat filtrování na základě typu přílohy zprávy tak, aby byly soubory určených typů automaticky přejmenovány nebo odstraněny. Přejmenováním přílohy určitého typu může aplikace Kaspersky Endpoint Security ochránit váš počítač před automatickým spuštěním škodlivé aplikace.

Postup konfigurace filtrování příloh:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V části **Filtr příloh** proveďte některou z následujících akcí:
   - Pokud nechcete, aby součást Ochrana před hrozbami v poště filtrovala přílohy zpráv, vyberte možnost **Zakázat filtrování**.
   - Chcete-li, aby součást Ochrana před hrozbami v poště přejmenovala přílohy zpráv určených typů, vyberte možnost **Přejmenovat přílohy vybraného typu**.
   - Pokud chcete, aby součást Ochrana před hrozbami v poště odstranila přípony zpráv určených typů souborů, vyberte možnost **Odstranit přílohy vybraného typu**.
5. Pokud jste v předchozím kroku vybrali možnost **Přejmenovat přílohy vybraného typu** nebo **Odstranit přílohy vybraného typu**, zaškrtněte políčka u odpovídajících typů souborů.
6. Uložte změny.

Export a import rozšíření pro filtrování příloh

Seznam přípon filtrů příloh můžete exportovat do souboru XML. Funkci exportu/importu můžete použít k zálohování seznamu rozšíření nebo k migraci seznamu na jiný server.

Jak exportovat a importovat seznam rozšíření filtru příloh v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
6. V části **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
7. V okně, které se otevře, vyberte kartu **Filtr příloh**.
8. Postup exportu seznamu rozšíření:
   a. Vyberte rozšíření, která chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam rozšíření, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam rozšíření do souboru XML.
9. Postup importu seznamu rozšíření:
   a. Klikněte na odkaz **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam rozšíření.
   c. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam rozšíření obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
10. Uložte změny.

Jak exportovat a importovat seznam rozšíření filtru příloh ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam výjimek.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
5. Postup exportu seznamu rozšíření v bloku **Filtr příloh**:
   a. Vyberte rozšíření, která chcete exportovat.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam rozšíření, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam rozšíření do souboru XML.
6. Postup importu seznamu rozšíření v bloku **Filtr příloh**:
   a. Klikněte na odkaz **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam rozšíření.
   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam rozšíření obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
7. Uložte změny.

Kontrola e-mailů v aplikaci Microsoft Office Outlook

Během instalace aplikace Kaspersky Endpoint Security se vloží rozšíření Ochrana před hrozbami v poště do aplikace Microsoft Office Outlook (dále je označovaná jako aplikace Outlook). Umožňuje otevřít nastavení součásti Ochrana před hrozbami v poště z aplikace Outlook a určit, kdy se mají e-maily kontrolovat na přítomnost virů a jiných hrozeb. Rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook umožňuje kontrolovat příchozí a odchozí zprávy přenášené přes protokoly POP3, SMTP, NNTP, IMAP a MAPI. Aplikace Kaspersky Endpoint Security také podporuje práci s dalšími e-mailovými klienty (včetně Microsoft Outlook Express®, Windows Mail a Mozilla™ Thunderbird™).

Rozšíření Ochrana před hrozbami v poště podporuje operace s aplikací Outlook 2010, 2013, 2016 a 2019.

Pokud používáte e-mailového klienta Mozilla Thunderbird, součást Ochrana před hrozbami v poště nebude kontrolovat přítomnost virů a jiných hrozeb ve zprávách přenášených prostřednictvím protokolu IMAP, pokud budou použity filtry k přesunu zpráv ze složky **doručené pošty**.

V aplikaci Outlook jsou příchozí zprávy nejprve zkontrolovány součástí Ochrana před hrozbami v poště (pokud je v rozhraní aplikace Kaspersky Endpoint Security zaškrtnuto políčko Kontrolovat přenosy POP3/SMTP/NNTP/IMAP) a potom rozšířením Ochrana před hrozbami v poště pro aplikaci Outlook. Pokud součást Ochrana před hrozbami v poště zjistí ve zprávě škodlivý objekt, na tuto událost vás upozorní.

Nastavení součásti Ochrana před hrozbami v poště lze provést přímo v aplikaci Outlook, pokud je v rozhraní aplikace Kaspersky Endpoint Security zaškrtnuto políčko Rozšíření aplikace Microsoft Outlook je připojeno.

Odchozí zprávy jsou nejprve zkontrolovány rozšířením Ochrana před hrozbami v poště pro aplikaci Outlook a potom součástí Ochrana před hrozbami v poště.

Pokud je e-mail kontrolován pomocí rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook, doporučujeme použít režim serveru Exchange s mezipamětí. Podrobnější informace o režimu serveru Exchange s mezipamětí a o doporučeních k jeho použití najdete ve znalostní bázi Microsoft Knowledge Base.

Postup konfigurace režimu operace rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook pomocí aplikace Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.
6. V části **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.

   Otevře se okno **Ochrana před hrozbami v poště**.
7. V části **Připojení** klikněte na tlačítko **Nastavení**.
8. V okně **Ochrana e-mailu**:
   - Pokud chcete, aby rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook kontrolovalo příchozí zprávy ihned po doručení do schránky, zaškrtněte políčko **Kontrola během příjmu**.
   - Pokud chcete, aby rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook kontrolovalo příchozí zprávy v okamžiku otevření uživatelem, zaškrtněte políčko **Kontrola během čtení**.
   - Pokud chcete, aby rozšíření Ochrana před hrozbami v poště pro aplikaci Outlook kontrolovalo odchozí zprávy v okamžiku odesílání, zaškrtněte políčko **Kontrola během odesílání**.
9. Uložte změny.

Ochrana před síťovými hrozbami

Součást Ochrana před síťovými hrozbami kontroluje příchozí síťový provoz a zjišťuje přítomnost aktivit typických pro síťové útoky. Pokud aplikace Kaspersky Endpoint Security zjistí pokus o útok na síť v počítači uživatele, zablokuje síťové připojení k útočícímu počítači.

Popisy aktuálně známých typů síťových útoků a způsoby, jak se jim bránit, jsou k dispozici v databázích aplikace Kaspersky Endpoint Security. Seznam síťových útoků, které je součást Ochrana před síťovými hrozbami schopna zjistit, se aktualizuje při aktualizacích databází a modulů aplikace.

Povolení a zakázání součásti Ochrana před síťovými hrozbami

Ve výchozím nastavení je součást Ochrana před síťovými hrozbami povolena a pracuje v optimálním režimu. V případě potřeby můžete součást Ochrana před síťovými hrozbami zakázat.

Postup povolení nebo zakázání součásti Ochrana před síťovými hrozbami:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Ochrana před síťovými hrozbami**.
3. Pomocí přepínače **Ochrana před síťovými hrozbami** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Je-li součást Ochrana před síťovými hrozbami povolena, aplikace Kaspersky Endpoint Security kontroluje v příchozím webovém provozu aktivitu typickou pro síťové útoky. Pokud aplikace Kaspersky Endpoint Security zjistí pokus o útok na síť v počítači uživatele, zablokuje síťové připojení k útočícímu počítači.

Blokování útočícího počítače

Postup zablokování útočícího počítače:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Ochrana před síťovými hrozbami**.
3. Zaškrtněte políčko **Přidat útočící počítač do seznamu blokovaných počítačů na N minut**.

   Pokud je toto políčko zaškrtnuto, přidá součást Ochrana před síťovými hrozbami útočící počítač do seznamu blokovaných počítačů. Znamená to, že součást Ochrana před síťovými hrozbami bude síťové propojení s útočícím počítačem blokovat po zadanou dobu od prvního pokusu o síťový útok. Takové blokování automaticky chrání počítač uživatele před možnými budoucími síťovými útoky ze stejné adresy.

   Seznam bloků můžete zobrazit v okně nástroje Sledování sítě.

   Aplikace Kaspersky Endpoint Security vymaže seznam bloků při svém restartu a při změně nastavení součásti Ochrana před síťovými hrozbami.

4. Časový interval, po který bude útočící počítač blokován, můžete změnit v poli vedle zaškrtávacího políčka **Přidat útočící počítač do seznamu blokovaných počítačů na N minut**.

5. Uložte změny.

Pokud aplikace Kaspersky Endpoint Security zjistí pokus o útok na síť v počítači uživatele, zablokuje všechna síťová připojení s útočícím počítačem.

Konfigurace adres výjimek z blokování

Aplikace Kaspersky Endpoint Security dokáže rozpoznat síťový útok a blokovat nezabezpečené síťové připojení, které přenáší velké množství paketů (například z bezpečnostních kamer). Chcete-li pracovat s důvěryhodnými zařízeními, můžete přidat IP adresy těchto zařízení do seznamu výjimek.

Postup konfigurace adres výjimek z blokování:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Ochrana před síťovými hrozbami**.

3. Klikněte na odkaz **Spravovat výjimky**.

4. V daném okně klikněte na tlačítko **Přidat**.

5. Zadejte IP adresu počítače, ze kterého nemají být blokovány síťové útoky.

6. Uložte změny.

Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu ze zařízení na seznamu výjimek.

Export a import seznamu výjimek z blokování

Seznam výjimek můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství adres stejného typu. Funkci exportu/importu můžete také použít k zálohování seznamu výjimek nebo k migraci seznamu na jiný server.

Jak exportovat a importovat seznam výjimek v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před síťovými hrozbami**.
6. V bloku **Nastavení Ochrany před síťovými hrozbami** klikněte na tlačítko **Výjimky**.
7. Postup exportu seznamu pravidel:
   a. Vyberte výjimky, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádnou výjimku nevybrali, aplikace Kaspersky Endpoint Security exportuje všechny výjimky.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
8. Postup importu seznamu výjimek:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
9. Uložte změny.

Jak exportovat a importovat seznam výjimek ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam výjimek.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Ochrana před síťovými hrozbami**.
5. V bloku **Nastavení Ochrany před síťovými hrozbami** klikněte na odkaz **Výjimky**.

   Otevře se seznam výjimek.
6. Postup exportu seznamu pravidel:
   a. Vyberte výjimky, které chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrďte, jestli chcete exportovat pouze vybrané výjimky, nebo exportovat celý seznam výjimek.
   d. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   e. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
7. Postup importu seznamu výjimek:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

Konfigurace ochrany proti síťovým útokům podle typu

Kaspersky Endpoint Security vám umožňuje spravovat ochranu před následujícími typy síťových útoků:

- *Přehlcení sítě* je útok na síťové zdroje organizace (například webové servery). Tento útok spočívá v odeslání velkého počtu požadavků za účelem přetížení šířky pásma síťových prostředků. Když k tomu dojde, uživatelé nebudou mít přístup k síťovým prostředkům organizace.
- Útoky typu *skenování portů* zahrnují skenování portů UDP, TCP a síťových služeb v počítači. Tento útok umožňuje útočníkovi určit stupeň zranitelnosti počítače před provedením nebezpečnějších typů síťových útoků.

Skenování portů také umožňuje útočníkovi identifikovat operační systém v počítači a vybrat vhodné síťové útoky pro tento operační systém.

- Součástí útoku *falšování adres MAC* je změna adresy MAC síťového zařízení (síťové karty). V důsledku toho může útočník přesměrovat data odeslaná do zařízení na jiné zařízení a získat přístup k těmto datům. Aplikace Kaspersky Endpoint Security umožňuje blokovat útoky falšování adres MAC a zobrazovat oznámení o útocích.

Detekci těchto typů útoků můžete zakázat v případě, že některé z vašich povolených aplikací provádějí operace, které jsou pro tyto typy útoků typické. To pomůže vyhnout se falešným poplachům.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security útoky typu přehlcení sítě, skenování portů a falšování adres MAC nesleduje.

Konfigurace ochrany proti síťovým útokům podle typu:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Ochrana před síťovými hrozbami**.
3. Chcete-li povolit nebo zakázat detekci těchto útoků, použijte přepínač **Považovat skenování portů a přehlcení sítě za útoky**.
4. Použijte přepínač **Ochrana před falšováním adresy MAC**.
5. V bloku **Při zjištění útoku falšování adres MAC** vyberte jednu z následujících možností:
   - **Pouze upozornit**.
   - **Upozornit a zablokovat**.
6. Uložte změny.

Brána firewall

Brána firewall blokuje neoprávněné připojení k počítači při práci na internetu nebo v místní síti. Brána firewall také řídí síťovou aktivitu aplikací v počítači. To vám umožní chránit vaši firemní LAN před krádeží identity a jinými útoky. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a předdefinovaných *pravidel sítě*.

Pro interakci s aplikací Kaspersky Security Center se používá síťový agent. Brána firewall automaticky vytváří pravidla sítě požadovaná pro fungování aplikace a síťového agenta. Díky tomu brána firewall otevírá několik portů v počítači. Které porty jsou otevřeny, závisí na roli počítače (například distribuční bod). Další informace o portech, které se budou v počítači otevírat, naleznete v *nápovědě k aplikaci Kaspersky Security Center*.

Pravidla sítě

Pravidla sítě můžete konfigurovat na následujících úrovních:

- *Pravidla síťových paketů*. Pravidla síťových paketů vytvářejí omezení pro síťové pakety bez ohledu na aplikaci. Takováto pravidla omezují příchozí a odchozí provoz konkrétních portů vybraného datového protokolu. Aplikace

Kaspersky Endpoint Security má předdefinovaná pravidla pro síťové pakety s oprávněními doporučenými odborníky společnosti Kaspersky.

- *pravidla sítě aplikace*. pravidla sítě aplikace vytvářejí omezení síťové aktivity konkrétní aplikace. Berou do úvahy nejen charakteristiky síťového paketu, ale také konkrétní aplikaci, které je síťový paket určen nebo která síťový paket vyslala.

Řízený přístup aplikací ke zdrojům, procesům a osobním údajům operačního systému umožňuje součást Prevence narušení hostitele pomocí *oprávnění aplikací*.

Při prvním spuštění aplikace provede brána firewall následující akce:

1. Zkontroluje zabezpečení aplikace pomocí stažených antivirových databází.
2. Zkontroluje zabezpečení webu ve službě Kaspersky Security Network.

   Doporučujeme vám zapojit se do služby Kaspersky Security Network, aby mohla tato služba fungovat ještě efektivněji.
3. Umístí aplikaci do jedné ze *skupin důvěryhodnosti*: Důvěryhodné, Nízké omezení, Vysoké omezení, Nedůvěryhodné.

   Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace. Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat.

   Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti pro součásti Brána firewall a Prevence narušení hostitele. Skupinu důvěryhodnosti nelze změnit pouze u součástí Brána firewall a Prevence narušení hostitele.

   Pokud jste účast v KSN odmítli nebo neexistuje žádná síť, aplikace Kaspersky Endpoint Security umístí aplikaci do skupiny důvěryhodnosti v závislosti na nastavení součásti Prevence narušení hostitele. Po obdržení reputace aplikace z KSN lze skupinu důvěryhodnosti změnit automaticky.
4. Blokuje síťovou aktivitu aplikace v závislosti na skupině důvěryhodnosti. Například aplikace ve skupině důvěrnosti s vysokým omezením nemohou používat žádná síťová připojení.

Při příštím spuštění aplikace ověří součást aplikace Kaspersky Endpoint Security integritu aplikace. Pokud je aplikace nezměněná, součást pro ni použije aktuální pravidla sítě. Pokud došlo ke změně aplikace, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spouštěna poprvé.

Priority pravidel sítě

Každé pravidlo má prioritu. Čím výše se pravidlo na seznamu nachází, tím vyšší je jeho priorita. Pokud je síťová aktivita přidána do několika pravidel, brána firewall ji reguluje podle pravidla s nejvyšší prioritou.

Pravidla síťových paketů mají vyšší prioritu než pravidla sítě pro aplikace. Pokud jsou pro stejný typ síťové aktivity určena pravidla síťových paketů i pravidla sítě pro aplikace, síťová aktivita bude zpracována podle pravidel síťových paketů.

pravidla sítě pro aplikace fungují následovně: pravidlo sítě pro aplikace zahrnuje pravidla přístupu založená na stavu sítě: *veřejná*, *místní* nebo *důvěryhodná*. Například aplikace ve skupině důvěryhodnosti s vysokým omezením nepovolují ve výchozím nastavení žádnou síťovou aktivitu v sítích všech stavů. Pokud je pro jednotlivé aplikace (nadřazenou aplikaci) zadáno pravidlo sítě, potom se podřízené procesy jiných aplikací spustí podle pravidla sítě nadřazené aplikace. Jestliže pro aplikaci neexistuje žádné pravidlo sítě, budou podřízené procesy spuštěny podle pravidla síťového přístupu skupiny důvěryhodnosti aplikace.

Například jste zakázali jakoukoli síťovou aktivitu v sítích všech stavů pro všechny aplikace s výjimkou prohlížeče X. Pokud spustíte instalaci prohlížeče Y (podřízený proces) z prohlížeče X (nadřazená aplikace), bude mít instalační program prohlížeče Y přístup k síti a stáhne si potřebné soubory. Po instalaci budou prohlížeči Y zamítnuta všechna síťová připojení podle nastavení brány firewall. Chcete-li zakázat síťovou aktivitu instalačního programu prohlížeče Y jako podřízený proces, musíte přidat pravidlo sítě pro instalační program tohoto prohlížeče.

Stavy síťového připojení

Brána firewall umožňuje řídit síťovou aktivitu v závislosti na stavu síťového připojení. Aplikace Kaspersky Endpoint Security přijímá stav síťového připojení z operačního systému počítače. Stav síťového připojení v operačním systému nastavuje uživatel při nastavování připojení. Stav síťového připojení můžete změnit v nastavení aplikace Kaspersky Endpoint Security. Brána firewall bude sledovat aktivitu sítě v závislosti na stavu sítě v nastavení aplikace Kaspersky Endpoint Security, a ne v operačním systému.

Síťové připojení může mít jeden z následujících typů stavu:

- **Veřejná síť**. Síť není chráněna antivirovými aplikacemi, bránami firewall ani filtry (například Wi-Fi v kavárně). Když uživatel používá počítač připojený k takovéto síti, brána firewall bude blokovat přístup k souborům a tiskárnám počítače. Externí uživatelé dále nebudou moci přistupovat k datům ve sdílených složkách a využívat vzdálený přístup k ploše počítače. Brána firewall filtruje síťovou aktivitu jednotlivých aplikací v závislosti na pravidlech sítě, které jsou pro ně nastaveny.

  Brána firewall ve výchozím nastavení přiřadí stav *Veřejná síť* například internetu. Stav v případě internetu nelze změnit.

- **Místní síť**. Síť pro uživatele s omezeným přístupem k souborům a tiskárnám v tomto počítači (například pro podnikovou síť LAN nebo domácí síť).

- **Důvěryhodná síť**. Bezpečná síť, ve které není počítač vystaven útokům nebo pokusům o neoprávněný přístup k datům. V rámci sítí s tímto stavem povolí brána firewall jakoukoli síťovou aktivitu.

Povolení a zakázání brány firewall

Ve výchozím nastavení je brána firewall povolena a pracuje v optimálním režimu.

Postup povolení nebo zakázání brány firewall:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Pomocí přepínače **Brána firewall** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Změna stavu připojení k síti

Brána firewall ve výchozím nastavení přiřadí stav *Veřejná síť* například internetu. Stav v případě internetu nelze změnit.

Postup změny stavu připojení k síti:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Dostupné sítě**.
4. Vyberte připojení k síti, jehož stav chcete změnit.
5. Ve sloupci **Typ sítě** vyberte stav síťového připojení:
   - **Veřejná síť**. Síť není chráněna antivirovými aplikacemi, bránami firewall ani filtry (například Wi-Fi v kavárně). Když uživatel používá počítač připojený k takovéto síti, brána firewall bude blokovat přístup k souborům a tiskárnám počítače. Externí uživatelé dále nebudou moci přistupovat k datům ve sdílených složkách a využívat vzdálený přístup k ploše počítače. Brána firewall filtruje síťovou aktivitu jednotlivých aplikací v závislosti na pravidlech sítě, které jsou pro ně nastaveny.
   - **Místní síť**. Síť pro uživatele s omezeným přístupem k souborům a tiskárnám v tomto počítači (například pro podnikovou síť LAN nebo domácí síť).
   - **Důvěryhodná síť**. Bezpečná síť, ve které není počítač vystaven útokům nebo pokusům o neoprávněný přístup k datům. V rámci sítí s tímto stavem povolí brána firewall jakoukoli síťovou aktivitu.
6. Uložte změny.

Správa pravidel síťových paketů

Při správě pravidel síťových paketů můžete provádět následující akce:

- Vytvořit nové pravidlo síťových paketů.

  Nové pravidlo síťových paketů můžete vytvořit vytvořením sady podmínek a akcí, které budou použity pro síťové pakety a datové toky.

- Povolit nebo zakázat pravidlo síťových paketů.

  Všechna pravidla síťových paketů vytvořená ve výchozím nastavení branou firewall mají stav *Povoleno*. Když je pravidlo síťových paketů povoleno, brána firewall bude pravidlo používat.

  Kterékoli pravidlo vybrané v seznamu pravidel síťových paketů můžete zakázat. Když je pravidlo síťových paketů zakázáno, brána firewall pravidlo dočasně nebude používat.

  > Ve výchozím nastavení je nové vlastní pravidlo síťových paketů přidáno do seznamu se stavem *Povoleno*.

- Upravit nastavení existujícího pravidla síťových paketů.

Po vytvoření nového pravidla síťových paketů se můžete kdykoli vrátit k jeho nastavení a podle potřeby ho upravit.

- Změnit akci brány firewall pro pravidlo síťových paketů.

  V seznamu pravidel síťových paketů můžete upravit akci, kterou provede brána firewall při zjištění síťové aktivity shodné s konkrétním pravidlem síťových paketů.

- Změnit prioritu pravidla síťových paketů.

  Můžete snížit nebo zvýšit prioritu pravidla síťových paketů vybraného v seznamu.

- Odebrat pravidlo síťových paketů.

  Pravidlo síťových paketů můžete odstranit, aby ho brána firewall nepoužívala při zjištění síťové aktivity a aby se toto pravidlo nezobrazovalo v seznamu pravidel síťových paketů se stavem *Zakázáno*.

Vytváření pravidla síťových paketů

Pravidlo síťových paketů můžete vytvořit následujícími způsoby:

- Použijte nástroj Sledování sítě.

  Sledování sítě je nástroj navržený k zobrazování informací o síťové aktivitě uživatelského počítače v reálném čase. To je výhodné, protože nemusíte konfigurovat všechna nastavení pravidel. Některá nastavení brány firewall budou vložena automaticky z dat Sledování sítě. Sledování sítě je k dispozici pouze v rozhraní aplikace.

- Nakonfigurujte nastavení brány firewall.

  To vám umožní doladit nastavení brány firewall. Můžete vytvořit pravidla pro jakoukoli síťovou aktivitu, i když v současné době není žádná síťová aktivita.

Při vytváření pravidel síťových paketů mějte na paměti, že mají vyšší prioritu než pravidla sítě pro aplikace.

Jak pomocí nástroje Sledování sítě vytvořit pravidlo síťových paketů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Sledování sítě**.
2. Vyberte kartu **Síťová aktivita**.

   Na kartě **Síťová aktivita** se zobrazují všechny aktuálně aktivní síťová připojení v počítači. Zobrazují se jak odchozí, tak příchozí síťová připojení.
3. V místní nabídce síťového připojení vyberte možnost **Vytvořit pravidlo paketů**.

   Tím otevřete vlastnosti pravidla sítě.
4. Nastavte pro pravidlo paketu stav **Aktivní**.
5. Do pole **název** ručně zadejte název síťové služby.
6. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Šablona pravidla sítě**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

   Všechna nastavení pravidel sítě budou vyplněna automaticky.
7. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
8. Klikněte na tlačítko **Uložit**.

   Nové pravidlo sítě bude přidáno do seznamu.
9. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
10. Uložte změny.

Jak pomocí nastavení brány firewall vytvořit pravidlo síťových paketů v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla paketů**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
4. Klikněte na tlačítko **Přidat**.

   Tím otevřete vlastnosti pravidla sítě.
5. Nastavte pro pravidlo paketu stav **Aktivní**.
6. Do pole **název** ručně zadejte název síťové služby.
7. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Šablona pravidla sítě**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

   Všechna nastavení pravidel sítě budou vyplněna automaticky.
8. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
9. Klikněte na tlačítko **Uložit**.

   Nové pravidlo sítě bude přidáno do seznamu.
10. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
11. Uložte změny.

Jak vytvořit pravidlo síťových paketů v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
6. V části **Nastavení brány firewall** klikněte na tlačítko **Nastavení**.

   Tím otevřete seznam pravidel síťových paketů a seznam pravidel sítě aplikací.
7. Vyberte kartu **Pravidla síťových paketů**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
8. Klikněte na tlačítko **Přidat**.

   Tím otevřete vlastnosti pravidla paketu.
9. Do pole **název** ručně zadejte název síťové služby.
10. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

    Předdefinovanou šablonu pravidla můžete vybrat kliknutím na tlačítko . Šablony pravidel popisují nejčastěji používaná síťová připojení.

    Všechna nastavení pravidel sítě budou vyplněna automaticky.
11. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
12. Klikněte na tlačítko **Uložit**.

    Nové pravidlo sítě bude přidáno do seznamu.
13. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
14. Uložte změny.

Brána firewall bude řídit síťové pakety podle daného pravidla. Pravidlo paketu můžete z provozu brány firewall deaktivovat, aniž byste jej odstranili ze seznamu. Chcete-li tak učinit, zrušte zaškrtnutí políčka vedle objektu.

Jak vytvořit pravidlo síťových paketů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
5. V bloku **Nastavení brány firewall** klikněte na odkaz **Pravidla síťových paketů**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
6. Klikněte na tlačítko **Přidat**.

   Tím otevřete vlastnosti pravidla paketu.
7. Do pole **název** ručně zadejte název síťové služby.
8. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Vybrat šablonu**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

   Všechna nastavení pravidel sítě budou vyplněna automaticky.
9. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
10. Klikněte na tlačítko **Uložit**.

    Nové pravidlo sítě bude přidáno do seznamu.
11. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
12. Uložte změny.

Brána firewall bude řídit síťové pakety podle daného pravidla. Pravidlo paketu můžete z provozu brány firewall deaktivovat, aniž byste jej odstranili ze seznamu. Pomocí přepínače ve sloupci **Stav** pravidlo paketů povolíte nebo zakážete.

Nastavení pravidla síťových paketů

Parametr	Popis
Akce	**Povolit**. **Blokovat**. **Podle pravidel aplikace**. Pokud je vybrána tato možnost, brána firewall použije na síťové připojení pravidla sítě aplikace.
Protokol	Aktivitu v síti můžete regulovat přes vybraný protokol: TCP, UDP, ICMP, ICMPv6, IGMP a GRE. Pokud je vybrán protokol ICMP nebo ICMPv6, můžete definovat typ paketu a kód ICMP. Pokud je vybrán typ protokolu TCP nebo UDP, můžete zadat čísla portů oddělená čárkou pro místní a vzdálené počítače, jejichž propojení má být sledováno.
Směr	**Příchozí (paket)**. Brána firewall použije pravidlo sítě na všechny příchozí síťové pakety. **Příchozí**. Brána firewall použije pravidlo sítě na všechny síťové pakety odesílané prostřednictvím připojení, které bylo iniciováno vzdáleným počítačem.

	Příchozí/odchozí. Brána firewall použije pravidlo sítě na příchozí a odchozí síťové pakety bez ohledu na to, zda bylo síťové připojení iniciováno uživatelským nebo vzdáleným počítačem. **Odchozí (paket)**. Brána firewall použije pravidlo sítě na všechny odchozí síťové pakety. **Odchozí**. Brána firewall použije síť pravidlo na všechny síťové pakety odesílané prostřednictvím připojení iniciovaného počítačem uživatele. Připojení naváže protokol TCP. Pro protokol TCP použijte směry **Příchozí**, **Odchozí** a **Příchozí/odchozí**. Všechny ostatní protokoly nenavazují připojení, ale odesílají pakety. U všech ostatních protokolů použijte směry **Příchozí (paket)**, **Odchozí (paket)** a **Příchozí/odchozí**.
Síťové adaptéry	Síťové adaptéry, které mohou odesílat nebo přijímat síťové pakety. Zadání nastavení síťových adaptérů umožňuje odlišit síťové pakety odeslané nebo přijaté síťovými adresami s totožnými IP adresami.
Doba života (TTL)	Omezte kontrolu síťových paketů na základě jejich doby životnosti (TTL).
Vzdálené adresy	Síťové adresy vzdálených počítačů, které mohou odesílat a přijímat síťové pakety. Brána firewall použije pravidlo sítě na zadaný rozsah vzdálených síťových adres. Do pravidla sítě můžete zahrnout všechny IP adresy, vytvořit samostatný seznam IP adres nebo vybrat podsíť (Důvěryhodné sítě, Místní sítě, Veřejné sítě).
Místní adresy	Síťové adresy počítačů, které mohou odesílat a přijímat síťové pakety. Brána firewall použije pravidlo sítě na zadaný rozsah místních síťových adres. Můžete zahrnout všechny IP adresy do pravidla sítě nebo vytvořit samostatný seznam IP adres. Občas není možné získat místní adresy pro aplikace. V takovém případě je tento parametr ignorován.

Povolení a zakázání pravidla síťových paketů

Postup povolení nebo zakázání pravidla síťových paketů:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla paketů**.
   Tím otevřete seznam výchozích pravidel síťových paketů, která jsou nastavena pro bránu firewall.
4. Vyberte požadované pravidlo síťových paketů ze seznamu.
5. Pomocí přepínače ve sloupci **Stav** pravidlo povolíte nebo zakážete.
6. Uložte změny.

Změna akce brány firewall pro pravidlo síťových paketů

Postup změny akce brány firewall pro pravidlo síťových paketů:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla paketů**.

   Tím otevřete seznam výchozích pravidel síťových paketů, která jsou nastavena pro bránu firewall.
4. Vyberte ji v seznamu pravidel síťových paketů a klikněte na tlačítko **Upravit**.
5. V rozevíracím seznamu **Akce** vyberte akci, kterou má provést brána firewall při zjištění tohoto druhu síťové aktivity:

   - **Povolit**.
   - **Blokovat**.
   - **Podle pravidel aplikace**.
6. Uložte změny.

Změna priority pravidla síťových paketů

Priorita pravidla síťových paketů je určena jeho polohou v seznamu pravidel síťových paketů. Pravidlo, které je nejvýše v seznamu pravidel síťových paketů, má nejvyšší prioritu.

Každé ručně vytvořené pravidlo síťových paketů je přidáno na konec seznamu a má nejnižší prioritu.

Brána firewall vykonává pravidla v pořadí, ve kterém se zobrazují v seznamu, od nejvyšší pozice k nejnižší. V závislosti na každém zpracovaném pravidle síťových paketů, které se vztahuje ke konkrétnímu síťovému připojení, brána firewall povolí nebo zablokuje přístup k adrese a portu, které jsou určeny v nastavení tohoto síťového připojení.

Postup změny priority pravidla síťových paketů:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla paketů**.

   Tím otevřete seznam výchozích pravidel síťových paketů, která jsou nastavena pro bránu firewall.
4. Ze seznamu vyberte pravidlo síťových paketů, jehož prioritu chcete změnit.
5. Pomocí tlačítek **Nahoru** a **Dolů** přesuňte pravidlo síťových paketů na požadované místo v seznamu.
6. Uložte změny.

Export a import pravidel síťových paketů

Seznam pravidel síťových paketů můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství pravidel stejného typu. Můžete použít funkci exportu/importu k zálohování seznamu pravidel paketů nebo k migraci seznamu na jiný server.

Jak exportovat a importovat seznam pravidel síťových paketů v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
6. Postup exportu seznamu pravidel síťových paketů:
   a. Vyberte pravidla, která chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádné pravidlo nevybrali, aplikace Kaspersky Endpoint Security exportuje všechna pravidla.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
7. Postup importu seznamu pravidel síťových paketů:
   a. Klikněte na odkaz **Importovat**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

Jak exportovat a importovat seznam pravidel síťových paketů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam pravidel.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
5. Klikněte na odkaz **Pravidla síťových paketů**.
6. Postup exportu seznamu pravidel síťových paketů:
   a. Vyberte pravidla, která chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrďte, jestli chcete exportovat pouze vybraná pravidla, nebo exportovat celý seznam pravidel.
   d. Klikněte na tlačítko **Exportovat**.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML ve výchozí složce pro stahování.
7. Postup importu seznamu pravidel síťových paketů:
   a. Klikněte na odkaz **Importovat**.

      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

Správa pravidel sítě aplikací

Ve výchozím nastavení seskupuje aplikace Kaspersky Endpoint Security všechny aplikace nainstalované v počítači podle názvu dodavatele softwaru, jehož soubor či síťovou aktivitu monitoruje. Skupiny aplikací jsou dále kategorizovány do skupin důvěryhodnosti. Všechny aplikace a skupiny aplikací dědí vlastnosti z nadřazené skupiny: pravidla kontroly aplikací, pravidla sítě aplikace a jejich prioritu provedení.

Stejně jako součást Prevence narušení hostitele aplikuje součást Brána firewall ve výchozím nastavení pravidla sítě pro skupinu aplikací při filtrování síťové aktivity všech aplikací v rámci skupiny. Pravidla sítě skupiny aplikací definují oprávnění aplikací ve skupině pro přístup k různým síťovým připojením.

Ve výchozím nastavení vytvoří brána firewall sadu pravidel sítě pro každou skupinu aplikací, která je v počítači zjištěna aplikací Kaspersky Endpoint Security. Akci brány firewall, která bude použita na výchozí pravidla sítě skupiny aplikací, můžete změnit. Nemůžete upravovat, odstraňovat, zakazovat ani měnit prioritu výchozích pravidel sítě skupiny aplikací.

Můžete také vytvořit pravidlo sítě pro konkrétní aplikaci. Takové pravidlo bude mít vyšší prioritu než pravidlo sítě skupiny, do které aplikace patří.

Vytváření pravidla sítě aplikací

Ve výchozím nastavení je aktivita aplikace kontrolována pravidly sítě, která jsou definována pro skupinu důvěryhodnosti, do níž byla aplikace zařazena aplikací Kaspersky Endpoint Security při prvním spuštění. Pokud je to nutné, můžete pravidla sítě upravit pro celou skupinu důvěryhodnosti, pro jednotlivou aplikaci nebo pro skupinu aplikací v rámci skupiny důvěryhodnosti.

Ručně definovaná pravidla sítě mají vyšší prioritu než pravidla sítě, která byla určena pro skupinu důvěryhodnosti. Jinými slovy, pokud se ručně definovaná pravidla aplikace liší od pravidel aplikace určených pro skupinu důvěryhodností, brána firewall kontroluje aktivitu aplikace podle ručně definovaných pravidel pro aplikace.

Ve výchozím nastavení vytváří brána firewall pro každou aplikaci následující pravidla sítě:

- Jakákoli síťová aktivita v rámci důvěryhodných sítí.
- Jakákoli síťová aktivita v rámci místních sítí.
- Jakákoli síťová aktivita v rámci veřejných sítí.

Kaspersky Endpoint Security kontroluje síťovou aktivitu aplikací podle předdefinovaných pravidel sítě následujícím způsobem:

- Důvěryhodné a s nízkým omezením: veškerá síťová aktivita je povolena.
- S vysokým omezením a nedůvěryhodné: veškerá síťová aktivita je blokována.

Předdefinovaná pravidla aplikace nelze upravovat ani odstraňovat.

Pravidla sítě aplikace můžete vytvářet následujícími způsoby:

- Použijte nástroj Sledování sítě.

  Sledování sítě je nástroj navržený k zobrazování informací o síťové aktivitě uživatelského počítače v reálném čase. To je výhodné, protože nemusíte konfigurovat všechna nastavení pravidel. Některá nastavení brány firewall budou vložena automaticky z dat Sledování sítě. Sledování sítě je k dispozici pouze v rozhraní aplikace.

- Nakonfigurujte nastavení brány firewall.

  To vám umožní doladit nastavení brány firewall. Můžete vytvořit pravidla pro jakoukoli síťovou aktivitu, i když v současné době není žádná síťová aktivita.

Při vytváření pravidel sítě pro aplikace nezapomeňte, že pravidla síťových paketů mají přednost před pravidly sítě aplikace.

Jak používat nástroj Sledování sítě k vytvoření pravidla sítě aplikace v rozhraní aplikace

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Sledování sítě**.
2. Vyberte kartu **Síťová aktivita** nebo **Otevřené porty**.

   Na kartě **Síťová aktivita** se zobrazují všechny aktuálně aktivní síťová připojení v počítači. Zobrazují se jak odchozí, tak příchozí síťová připojení.

   Na kartě **Otevřené porty** jsou vypsány všechny otevřené síťové porty počítače.
3. V místní nabídce síťového připojení vyberte položku **Vytvořit pravidlo aplikací**.

   Otevře se okno pravidel a vlastností aplikace.
4. Vyberte kartu **Pravidla sítě**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
5. Klikněte na tlačítko **Přidat**.

   Tím otevřete vlastnosti pravidla sítě.
6. Do pole **název** ručně zadejte název síťové služby.
7. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Šablona pravidla sítě**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

   Všechna nastavení pravidel sítě budou vyplněna automaticky.
8. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
9. Klikněte na tlačítko **Uložit**.

   Nové pravidlo sítě bude přidáno do seznamu.
10. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
11. Uložte změny.

Jak používat nastavení brány firewall k vytvoření pravidla sítě aplikace v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla aplikace**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
4. V seznamu aplikací vyberte aplikaci nebo skupinu aplikací, pro kterou chcete vytvořit pravidlo sítě.
5. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku a vyberte položku **Podrobnosti a pravidla**.

   Otevře se okno pravidel a vlastností aplikace.
6. Vyberte kartu **Pravidla sítě**.
7. Klikněte na tlačítko **Přidat**.

   Tím otevřete vlastnosti pravidla sítě.
8. Do pole **název** ručně zadejte název síťové služby.
9. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Šablona pravidla sítě**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

   Všechna nastavení pravidel sítě budou vyplněna automaticky.
10. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
11. Klikněte na tlačítko **Uložit**.

    Nové pravidlo sítě bude přidáno do seznamu.
12. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.
13. Uložte změny.

Jak vytvořit pravidlo sítě aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
6. V části **Nastavení brány firewall** klikněte na tlačítko **Nastavení**.

   Tím otevřete seznam pravidel síťových paketů a seznam pravidel sítě aplikací.
7. Vyberte kartu **Pravidla sítě aplikací**.
8. Klikněte na tlačítko **Přidat**.
9. V okně, který se otevře, zadejte kritéria vyhledávání aplikací, pro něž chcete vytvořit pravidlo sítě.

   Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
10. Klikněte na tlačítko **Aktualizovat**.

    Aplikace Kaspersky Endpoint Security vyhledá aplikaci v konsolidovaném seznamu aplikací nainstalovaných na spravovaných počítačích. Aplikace Kaspersky Endpoint Security zobrazí seznam aplikací, které splňují vaše vyhledávací kritéria.
11. Vyberte požadovanou aplikaci.
12. V rozevíracím seznamu **Přidat vybrané aplikace do <skupina zabezpečení>** Rozevírací vyberte položku **Výchozí skupiny** a klikněte na tlačítko **OK**.

    Aplikace bude přidána do výchozí skupiny.
13. Vyberte příslušnou aplikaci a poté vyberte možnost **Oprávnění aplikací** v místní nabídce aplikace.

    Otevře se okno pravidel a vlastností aplikace.
14. Vyberte kartu **Pravidla sítě**.

    Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
15. Klikněte na tlačítko **Přidat**.

    Tím otevřete vlastnosti pravidla sítě.
16. Do pole **název** ručně zadejte název síťové služby.
17. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

    Předdefinovanou šablonu pravidla můžete vybrat kliknutím na tlačítko . Šablony pravidel popisují nejčastěji používaná síťová připojení.

    Všechna nastavení pravidel sítě budou vyplněna automaticky.
18. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
19. Klikněte na tlačítko **Uložit**.

Nové pravidlo sítě bude přidáno do seznamu.

20. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.

21. Uložte změny.

[Jak vytvořit pravidlo sítě aplikace ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
5. V bloku **Nastavení brány firewall** klikněte na odkaz **Pravidla sítě aplikací**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Vyberte kartu **Oprávnění aplikací**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.
7. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.
8. Klikněte na odkaz **Vybraná cílová skupina** a vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.
9. Vyberte typ **Aplikace**. Klikněte na tlačítko **Další**.

   Pokud chcete vytvořit pravidlo sítě pro více aplikací, vyberte typ **Skupina** a definujte název skupiny aplikací.
10. V seznamu aplikací, který se otevře, vyberte aplikace, pro něž chcete vytvořit pravidlo sítě.

    Použijte filtr. Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
11. Dokončete průvodce kliknutím na tlačítko **OK**.

    Aplikace bude přidána do skupiny důvěryhodnosti.
12. V levé části okna vyberte příslušnou aplikaci.
13. V pravé části okna vyberte z rozevíracího seznamu možnost **Pravidla sítě**.

    Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
14. Klikněte na tlačítko **Přidat**.

    Tím otevřete vlastnosti pravidla aplikace.
15. Do pole **název** ručně zadejte název síťové služby.
16. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

    Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Vybrat šablonu**. Šablony pravidel popisují nejčastěji používaná síťová připojení.

    Všechna nastavení pravidel sítě budou vyplněna automaticky.
17. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
18. Klikněte na tlačítko **Uložit**.

    Nové pravidlo sítě bude přidáno do seznamu.

19. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.

20. Uložte změny.

Nastavení pravidla sítě aplikace

Parametr	Popis
Akce	**Povolit**. **Blokovat**.
Protokol	Aktivitu v síti můžete regulovat přes vybraný protokol: TCP, UDP, ICMP, ICMPv6, IGMP a GRE. Pokud je vybrán protokol ICMP nebo ICMPv6, můžete definovat typ paketu a kód ICMP. Pokud je vybrán typ protokolu TCP nebo UDP, můžete zadat čísla portů oddělená čárkou pro místní a vzdálené počítače, jejichž propojení má být sledováno.
Směr	**Příchozí**. **Příchozí/odchozí**. **Odchozí**.
Vzdálené adresy	Síťové adresy vzdálených počítačů, které mohou odesílat a přijímat síťové pakety. Brána firewall použije pravidlo sítě na zadaný rozsah vzdálených síťových adres. Do pravidla sítě můžete zahrnout všechny IP adresy, vytvořit samostatný seznam IP adres nebo vybrat podsíť (Důvěryhodné sítě, Místní sítě, Veřejné sítě).
Místní adresy	Síťové adresy počítačů, které mohou odesílat a přijímat síťové pakety. Brána firewall použije pravidlo sítě na zadaný rozsah místních síťových adres. Můžete zahrnout všechny IP adresy do pravidla sítě nebo vytvořit samostatný seznam IP adres. Občas není možné získat místní adresy pro aplikace. V takovém případě je tento parametr ignorován.

Povolení a zakázání pravidla sítě aplikace

Postup povolení nebo zakázání pravidla sítě aplikace:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.

3. Klikněte na tlačítko **Pravidla aplikace**.
   Tím otevřete seznam pravidel aplikace.

4. V seznamu aplikací vyberte aplikaci nebo skupinu aplikací, pro kterou chcete vytvořit nebo upravit pravidlo sítě.

5. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku a vyberte položku **Podrobnosti a pravidla**.
   Otevře se okno pravidel a vlastností aplikace.

6. Vyberte kartu **Pravidla sítě**.

7. V seznamu pravidel sítě pro skupinu aplikací vyberte relevantní pravidlo sítě.

Otevře se okno vlastností pravidla sítě.

8. Nastavte pro pravidlo sítě stav **Aktivní** nebo **Neaktivní**.

   Výchozí pravidlo sítě skupiny aplikací vytvořené bránou firewall nelze zakázat.

9. Uložte změny.

Změna akce brány firewall pro pravidlo sítě aplikace

Můžete změnit akci brány firewall použitou na všechna výchozí pravidla sítě pro aplikaci nebo skupinu aplikací a nahradit akci brány firewall jedním vlastním pravidlem sítě pro aplikaci nebo skupinu aplikací.

Postup změny akce brány firewall pro všechna pravidla sítě aplikace nebo skupiny aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla aplikace**.

   Tím otevřete seznam pravidel aplikace.

4. Pokud chcete změnit akci brány firewall použitou na všechna výchozí pravidla sítě, vyberte v seznamu aplikaci nebo skupinu aplikací. Ručně vytvořená pravidla sítě budou ponechána beze změny.
5. Kliknutím pravým tlačítkem otevřete kontextovou nabídku, vyberte **Pravidla sítě** a poté vyberte akci, kterou chcete přiřadit:

   - **Dědit**.
   - **Povolit**.
   - **Blokovat**.

6. Uložte změny.

Postup změny reakce brány firewall pro jedno pravidlo sítě aplikace nebo skupiny aplikací.

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla aplikace**.

   Tím otevřete seznam pravidel aplikace.

4. V seznamu vyberte aplikaci nebo skupinu aplikací, u které chcete změnit akci pro jedno pravidlo sítě.
5. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku a vyberte položku **Podrobnosti a pravidla**.

   Otevře se okno pravidel a vlastností aplikace.

6. Vyberte kartu **Pravidla sítě**.
7. Vyberte pravidlo sítě, pro které chcete změnit akci brány firewall.

8. Kliknutím pravým tlačítkem myši do sloupce **Povolení** zobrazte kontextovou nabídku a vyberte akci, kterou chcete přiřadit:
   - **Dědit.**
   - **Povolit**.
   - **Blokovat**.
   - **Protokolovat události**.
9. Uložte změny.

Změna priority pravidla sítě aplikace

Priorita pravidla sítě je určena jeho polohou v seznamu pravidel sítě. Brána firewall vykonává pravidla v pořadí, ve kterém se zobrazují v seznamu, od nejvyšší pozice k nejnižší. V závislosti na každém zpracovaném pravidle sítě, které se vztahuje ke konkrétnímu síťovému připojení, brána firewall povolí nebo zablokuje přístup k adrese a portu, které jsou určeny v nastavení tohoto síťového připojení.

Ručně vytvořená pravidla sítě mají vyšší prioritu než výchozí pravidla sítě.

Nemůžete měnit prioritu výchozích pravidel sítě skupiny aplikací.

Postup změny priority pravidla sítě:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla aplikace**.
   Tím otevřete seznam pravidel aplikace.
4. V seznamu aplikací vyberte aplikaci nebo skupinu aplikací, pro které chcete změnit prioritu pravidla sítě.
5. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku a vyberte položku **Podrobnosti a pravidla**.
   Otevře se okno pravidel a vlastností aplikace.
6. Vyberte kartu **Pravidla sítě**.
7. Vyberte pravidlo sítě, jehož prioritu chcete změnit.
8. Pomocí tlačítek **Nahoru** a **Dolů** přesuňte pravidlo sítě na požadované místo v seznamu.
9. Uložte změny.

Sledování sítě

Sledování sítě je nástroj navržený k zobrazování informací o síťové aktivitě uživatelského počítače v reálném čase.

Postup spuštění součásti Sledování sítě:

V hlavním okně aplikace klikněte na **Další nástroje** → **Sledování sítě**.

Otevře se okno **Sledování sítě**. V tomto okně se zobrazují informace o síťové činnosti počítače na čtyřech různých kartách:

- Na kartě **Síťová aktivita** se zobrazují všechny aktuálně aktivní síťová připojení v počítači. Zobrazují se jak odchozí, tak příchozí síťová připojení. Na této kartě můžete také vytvořit pravidla síťových paketů pro provoz brány firewall.
- Na kartě **Otevřené porty** jsou vypsány všechny otevřené síťové porty počítače. Na této kartě můžete také vytvořit pravidla síťových paketů a pravidla aplikací pro provoz brány firewall.
- Na kartě **Síťový provoz** se zobrazují informace o objemu příchozího a odchozího síťového provozu mezi počítačem uživatele a jinými počítači v síti, k nimž je uživatel aktuálně připojený.
- Na kartě **Blokované počítače** se zobrazují IP adresy vzdálených počítačů, jejichž síťová činnost byla zablokována součástí Ochrana před síťovými hrozbami po zjištění pokusů o síťový útok z takových IP adres.

Ochrana před útoky BadUSB

Některé viry mohou pozměnit firmware zařízení USB, aby ho operační systém omylem rozpoznal jako klávesnici. Virus tak může pod vaším uživatelským účtem provádět příkazy, které například stahují malware.

Součást Ochrana před útoky BadUSB brání tomu, aby se infikovaná zařízení USB napodobující klávesnici připojila k počítači.

Když je zařízení USB připojeno k počítači a identifikováno operačním systémem jako klávesnice, aplikace vyzve uživatele k zadání číselného kódu vygenerovaného aplikací pomocí této klávesnice nebo pomocí klávesnice na obrazovce (viz obrázek níže). Tento postup je známý jako autorizace klávesnice.

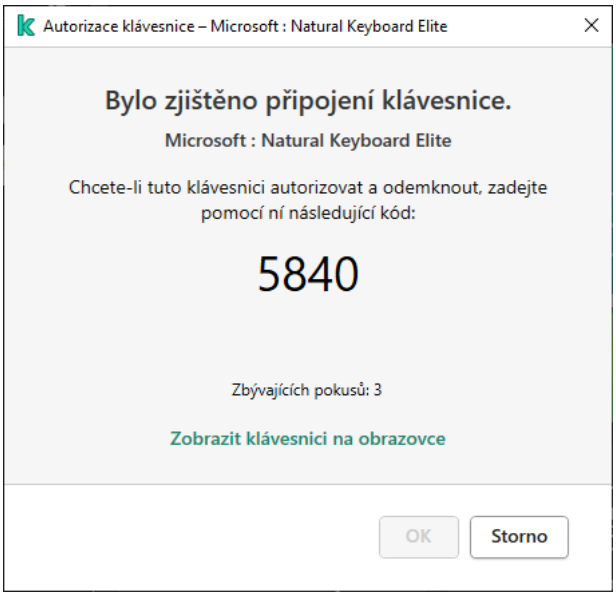
Pokud byl kód zadán správně, aplikace uloží parametry identifikace (kódy VID/PID klávesnice a číslo portu, ke kterému byla připojena) do seznamu autorizovaných klávesnic. Autorizaci není třeba opakovat po opětovném připojení klávesnice ani po restartování operačního systému.

Když autorizovanou klávesnici připojíte k jinému portu USB počítače, aplikace zobrazí výzvu k autorizaci této klávesnice znovu.

Pokud číselný kód zadáte nesprávně, aplikace vygeneruje nový kód. Na zadání číselného kódu máte tři pokusy. Pokud číselný kód zadáte nesprávně třikrát za sebou nebo okno **Autorizace klávesnice <Název klávesnice>** zavřete, aplikace vstup z této klávesnice zablokuje. Pokud klávesnici odpojíte a znovu připojíte nebo restartujete operační systém, aplikace vás k autorizaci klávesnice vyzve znovu.

Aplikace dovolí použití autorizované klávesnice a zablokuje klávesnici, která nebyla autorizována.

Součást Ochrana před útoky BadUSB není ve výchozím nastavení nainstalována. Pokud součást Ochrana před útoky BadUSB potřebujete, můžete ji přidat do vlastností instalačního balíčku před instalací aplikace nebo změnit dostupné komponenty aplikace po instalaci aplikace.



Autorizace klávesnice

Povolení a zakázání součásti Ochrana před útoky BadUSB

Zařízení USB, která byla operačním systémem identifikována jako klávesnice a jsou připojena před instalací součásti Ochrana před útoky BadUSB, budou po instalaci součásti považována za autorizovaná.

Postup povolení nebo zakázání součásti Ochrana před útoky BadUSB:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Základní ochrana před hrozbami → Ochrana před útoky BadUSB**.
3. Pomocí přepínače **Ochrana před útoky BadUSB** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je povolena součást Ochrana před útoky BadUSB, vyžaduje aplikace Kaspersky Endpoint Security autorizaci připojeného zařízení USB, které operační systém identifikuje jako klávesnici. Uživatel nemůže neautorizovanou klávesnici používat, dokud nebude autorizována.

Zakázání používání klávesnice na obrazovce k autorizaci zařízení USB

Klávesnice na obrazovce by měla být použita pouze k autorizaci zařízení USB, která nepodporují zadávání náhodných znaků (např. čtečka čárových kódů). Klávesnici na obrazovce nedoporučujeme používat k autorizaci neznámých zařízení USB.

Postup povolení nebo zakázání použití klávesnice na obrazovce k autorizaci:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Základní ochrana před hrozbami → Ochrana před útoky BadUSB**.

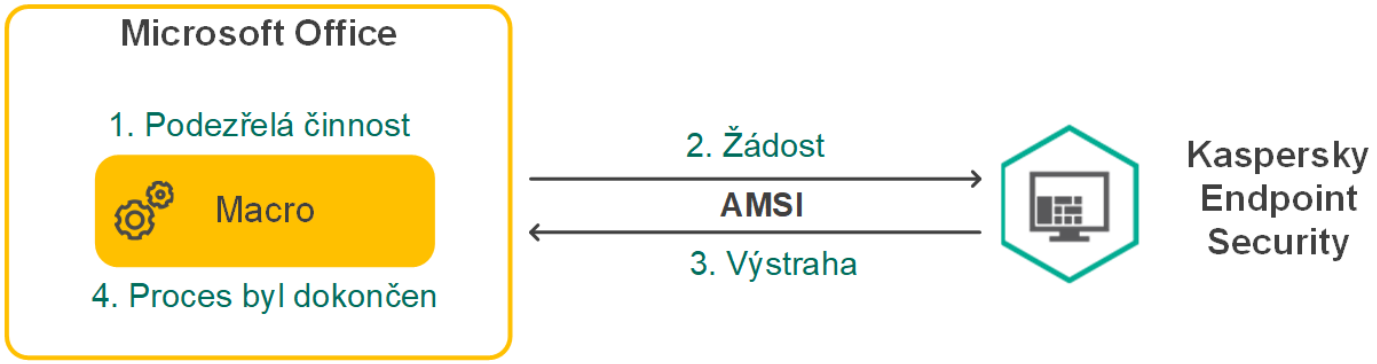
3. Prostřednictvím políčka **Zakázat klávesnici na obrazovce pro ověřování zařízení USB** můžete blokovat nebo povolit používání klávesnice na obrazovce k autorizaci.

4. Uložte změny.

Ochrana AMSI

Součást Ochrana AMSI je určen k podpoře rozhraní Antimalware Scan Interface od společnosti Microsoft. *Rozhraní AMSI (Antimalware Scan Interface)* umožňuje aplikacím třetích stran s podporou rozhraní AMSI odesílat objekty (například skripty prostředí PowerShell) do aplikace Kaspersky Endpoint Security za účelem další kontroly a přijímat výsledky kontroly těchto objektů. Aplikace třetích stran mohou zahrnovat například aplikace Microsoft Office (viz obrázek níže). Podrobnosti o rozhraní AMSI najdete v *dokumentaci společnosti Microsoft*.

Ochrana AMSI může pouze zjistit hrozby v aplikaci třetí strany a upozornit na ně, ale nemůže hrozby zpracovat. Aplikace třetí strany po obdržení oznámení týkající se hrozby nepovolí provedení škodlivých akcí (například se ukončí).



Příklad fungování AMSI

Ochrana AMSI může odmítnout žádost od aplikace třetí strany, a to například v případě, že tato aplikace překročí maximální počet žádostí v zadaném intervalu. Aplikace Kaspersky Endpoint Security odešle administračnímu serveru informace o odmítnuté žádosti od aplikace třetí strany. Součást Ochrana AMSI neodmítne žádosti od těchto aplikací třetích stran, u kterých je zaškrtnuto políčko **Neblokovat interakci se součástí Ochrana AMSI**.

Ochrana AMSI je k dispozici pro následující operační systémy pro pracovní stanice a servery:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Povolení a zakázání součásti Ochrana AMSI

Součást Ochrana AMSI je ve výchozím nastavení povolena.

Postup povolení nebo zakázání součásti Ochrana AMSI:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana AMSI**.
3. Pomocí přepínače **Ochrana AMSI** povolte nebo zakažte příslušnou součást.
4. Uložte změny.

Používání ochrany AMSI ke kontrole složených souborů

Běžnou technikou pro skrývání virů a jiného malwaru je jejich vkládání do složených souborů, například do archivů. Aby bylo možné zjistit viry a jiný malware skrytý tímto způsobem, složený soubor musí být rozbalen, což může zpomalit kontrolu. Kontrolu můžete zrychlit omezením typů složených souborů určených ke kontrole.

Postup konfigurace kontroly součástí Ochrana AMSI:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Základní ochrana před hrozbami** → **Ochrana AMSI**.
3. V části **Kontrola složených souborů** zadejte typy složených souborů, které chcete kontrolovat: archivy, distribuční balíček nebo soubory ve formátech sady Office.
4. V části **Omezení velikosti** proveďte jednu z následujících akcí:
   - Chcete-li zakázat, aby součást Ochrana AMSI rozbalovala velké složené soubory, zaškrtněte políčko **Nerozbalovat velké složené soubory** a zadejte požadovanou hodnotu do pole **Maximální velikost souboru**. Součást Ochrana AMSI nebude rozbalovat velké složené soubory překračující zadanou velikost.
   - Chcete-li povolit, aby součást Ochrana AMSI rozbalovala velké složené soubory, zrušte zaškrtnutí políčka **Nerozbalovat velké složené soubory**.

   Součást Ochrana AMSI kontroluje velké soubory extrahované z archivů bez ohledu na to, zda je či není zaškrtnuto políčko **Nerozbalovat velké složené soubory**.
5. Uložte změny.

Prevence zneužití

Součást Prevence zneužití detekuje programový kód, který využívá chyb zabezpečení v počítači k zneužití oprávnění správce nebo k provádění škodlivých činností. Zneužití může například využít útok v podobě přetečení vyrovnávací paměti. Za tímto účelem útočník odešle do zranitelné aplikace velké množství dat. Při zpracování těchto dat zranitelná aplikace spustí škodlivý kód. V důsledku tohoto útoku může útočník spustit neoprávněnou instalaci malwaru.

Pokud dojde k pokusu o spuštění spustitelného souboru ze zranitelné aplikace, které neprovedl uživatel, aplikace Kaspersky Endpoint Security spuštění tohoto souboru zablokuje nebo informuje uživatele.

Povolení a zakázání součásti Prevence zneužití

Ve výchozím nastavení je součást Prevence zneužití povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. V případě potřeby můžete součást Prevence zneužití zakázat.

Postup povolení nebo zakázání součásti Prevence zneužití:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence zneužití**.
3. Pomocí přepínače **Prevence zneužití** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je povolena součást Prevence zneužití, aplikace Kaspersky Endpoint Security monitoruje spuštěné soubory spouštěné zranitelnými aplikacemi. Pokud aplikace Kaspersky Endpoint Security zjistí, že spustitelný soubor ze zranitelné aplikace nebyl spuštěn uživatelem, ale jiným způsobem, aplikace Kaspersky Endpoint Security provede vybranou akci (například zablokuje operaci).

Výběr akce, která se má provést při zjištění zneužití

Ve výchozím nastavení bude aplikace Kaspersky Endpoint Security při zjištění zneužití blokovat operace, které jsou při pokusu o zneužití prováděny.

Výběr akce, která se má provést při zjištění zneužití:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence zneužití**.
3. V bloku **Při zjištění zneužití** vyberte příslušnou akci:
   - **Blokovat akci**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při zjištění zneužití zablokuje operace tohoto zneužití a vytvoří položku protokolu s informacemi o tomto zneužití.
   - **Informovat**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při zjištění zneužití uloží do protokolu položku obsahující informace o zneužití a přidá informace o tomto zneužití do seznamu aktivních hrozeb.
4. Uložte změny.

Ochrana paměti systémových procesů

Ve výchozím nastavení je ochrana paměti systémových procesů povolená.

Postup povolení nebo zakázání ochrany paměti systémových procesů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Rozšířená ochrana před hrozbami → Prevence zneužití**.
3. Chcete-li povolit nebo zakázat tuto funkci, použijte přepínač **Povolit ochranu paměti systémových procesů**.
4. Uložte změny.

Aplikace Kaspersky Endpoint Security bude blokovat externí procesy, které se pokoušejí získat přístup k systémovým procesům.

Detekce chování

Součást Detekce chování přijímá data o akcích aplikací v počítači a tyto informace poskytuje jiným součástem ochrany, což zvyšuje jejich výkon.

Součást Detekce chování využívá podpisy BSS (Behavior Stream Signatures) pro aplikace. Pokud se činnost aplikace shoduje s podpisem BSS, aplikace Kaspersky Endpoint Security provede vybranou reaktivní akci. Fungování aplikace Kaspersky Endpoint Security na základě podpisů BSS poskytuje aktivní ochranu počítače.

Povolení a zakázání součásti Detekce chování

Ve výchozím nastavení je součást Detekce chování povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. V případě potřeby můžete součást Detekce chování zakázat.

Zakázání součásti Detekce chování nedoporučujeme, pokud to není nezbytně nutné, protože by se tím snížila účinnost součástí ochrany. Součásti ochrany mohou vyžadovat data shromážděná součástí Detekce chování za účelem zjištění hrozeb.

Postup povolení nebo zakázání součásti Detekce chování:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Rozšířená ochrana před hrozbami → Detekce chování**.
3. Pomocí přepínače **Detekce chování** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je součást Detekce chování povolena, aplikace Kaspersky Endpoint Security bude pomocí podpisů BSS analyzovat aktivitu aplikací v operačním systému.

Výběr akce, která se má provést při zjištění aktivity malwaru

Chcete-li vybrat, jaká akce se má provést, pokud je aplikace zapojena do škodlivé činnosti, proveďte následující postup:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Detekce chování**.
3. Vyberte příslušnou akci v bloku **Při detekci nebezpečné aktivity**:
   - **Odstranit soubor**. V případě, že je vybrána tato položka, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity odstraní spustitelný soubor škodlivého programu a vytvoří ve složce záloh jeho záložní kopii.
   - **Ukončit aplikaci**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity ukončí tuto aplikaci.
   - **Informovat**. Pokud je vybrána tato položka a je zjištěna škodlivá aktivita aplikace, aplikace Kaspersky Endpoint Security přidá informace o škodlivé aktivitě aplikace do seznamu aktivních hrozeb.
4. Uložte změny.

Ochrana sdílených složek proti externímu šifrování

Součást sleduje operace provedené pouze se soubory, které jsou uloženy na velkokapacitních paměťových zařízeních se souborovým systémem NTFS a které nejsou šifrovány systémem EFS.

Ochrana sdílených složek proti externímu šifrování poskytuje analýzu aktivity ve sdílených složkách. Pokud se tato aktivita shoduje se signaturou chování datového proudu, které je typické pro externí šifrování, aplikace Kaspersky Endpoint Security provede vybranou akci.

Ve výchozím nastavení je ochrana sdílených složek proti externímu šifrování vypnutá.

Po nainstalování aplikace Kaspersky Endpoint Security bude fungování ochrany sdílených složek proti externímu šifrování omezené, dokud nebude počítač restartován.

Povolení a zakázání ochrany sdílených složek proti externímu šifrování

Po nainstalování aplikace Kaspersky Endpoint Security bude fungování ochrany sdílených složek proti externímu šifrování omezené, dokud nebude počítač restartován.

Postup povolení nebo zakázání ochrany sdílených složek proti externímu šifrování:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Detekce chování**.
3. Pomocí přepínače **Povolit ochranu sdílených složek proti externímu šifrování** můžete povolit nebo zakázat detekci aktivity, která je typická pro externí šifrování.

4. Uložte změny.

Výběr akce, která se má provést při zjištění externího šifrování sdílených složek

Postup výběru akce, která se má provést při zjištění externího šifrování sdílených složek:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Detekce chování**.
3. V části **Ochrana sdílených složek proti externímu šifrování** vyberte příslušnou akci:
   - **Blokovat připojení po dobu N min**. Pokud je tato možnost vybrána a aplikace Kaspersky Endpoint Security zjistí pokus o úpravu souborů ve sdílených složkách, provede následující akce:
     - Blokuje síťovou aktivitu počítače při pokusu o změnu.
     - Vytvoří záložní kopie souborů, které jsou upravovány.
     - Přidá položku do zpráv místního aplikačního rozhraní.
     - Odešle informace o zjištěné škodlivé aktivitě aplikaci Kaspersky Security Center.

     Pokud je povolena součást Modul pro nápravu, upravené soubory jsou obnoveny ze záložních kopií.
   - **Informovat**. Pokud je tato možnost vybrána a aplikace Kaspersky Endpoint Security zjistí pokus o úpravu souborů ve sdílených složkách, provede následující akce:
     - Přidá položku do zpráv místního aplikačního rozhraní.
     - Přidá položku do seznamu aktivních hrozeb.
     - Odešle informace o zjištěné škodlivé aktivitě aplikaci Kaspersky Security Center.
4. Uložte změny.

Vytvoření výjimky pro ochranu sdílených složek proti externímu šifrování

Výjimka u složky může snížit počet falešně pozitivních výsledků, pokud vaše organizace používá při výměně souborů pomocí sdílených složek šifrování dat. Součást Detekce chování může například vyvolat falešné poplachy, pokud uživatel pracuje se soubory s příponou ENC ve sdílené složce. Tato činnost odpovídá vzorci chování, který je typický pro externí šifrování. Pokud jste ve sdílené složce zašifrovali soubory za účelem ochrany dat, přidejte tuto složku do výjimek.

Jak vytvořit výjimku pro ochranu sdílených složek pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Obecná nastavení** → **Výjimky**.
6. V části **Výjimky z kontroly a důvěryhodné aplikace** klikněte na tlačítko **Nastavení**.
7. V okně, které se otevře, vyberte kartu **Výjimky z kontroly**.

   Otevře se okno obsahující seznam výjimek z kontroly.
8. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy výjimek v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Výjimky z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna ani odstranění výjimky v nadřazené zásadě nejsou možné.
9. Pokud chcete uživateli umožnit vytvoření místního seznamu výjimek, zaškrtněte políčko **Povolit používání místních důvěryhodných aplikací**. Tímto způsobem může uživatel kromě obecného seznamu výjimek z kontroly generovaného v zásadách vytvořit svůj vlastní místní seznam výjimek z kontroly. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu výjimek z kontroly generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené soubory z kontroly.
10. Klikněte na tlačítko **Přidat**.
11. V části **Vlastnosti** zaškrtněte políčko **Soubor nebo složka**.
12. Kliknutím na odkaz **Vybrat soubor nebo složku** v části **Popis výjimky z kontroly (podtržené položky můžete po kliknutí upravovat)** otevřete okno **Název souboru nebo složky**.
13. Klikněte na tlačítko **Procházet** a vyberte sdílenou složku.

    Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`:

    - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
    - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Složka` kromě této složky `Složka` samotné. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.

- Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.

14. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

15. Kliknutím na **jakýkoli** odkaz v části **Popis výjimky z kontroly (podtržené položky můžete po kliknutí upravovat)** aktivujte odkaz pro **výběr součástí**.

16. Kliknutím na odkaz **Vyberte komponenty** otevřete okno **Součásti ochrany**.

17. Zaškrtněte políčko vedle složky **Detekce chování**.

18. Uložte změny.

[Jak vytvořit výjimku pro ochranu sdílených složek pomocí webové konzoly a cloudové konzoly](#)

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Obecná nastavení** → **Výjimky**.
5. V bloku **Výjimky z kontroly a důvěryhodné aplikace** klikněte na odkaz **Výjimky z kontroly**.
6. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy výjimek v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Výjimky z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna ani odstranění výjimky v nadřazené zásadě nejsou možné.
7. Pokud chcete uživateli umožnit vytvoření místního seznamu výjimek, zaškrtněte políčko **Povolit používání místních důvěryhodných aplikací**. Tímto způsobem může uživatel kromě obecného seznamu výjimek z kontroly generovaného v zásadách vytvořit svůj vlastní místní seznam výjimek z kontroly. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu výjimek z kontroly generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené soubory z kontroly.
8. Klikněte na tlačítko **Přidat**.
9. Vyberte, jak chcete výjimku přidat: **Soubor nebo složka**.
10. Klikněte na tlačítko **Procházet** a vyberte sdílenou složku.

    Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`:

    - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
    - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Složka` kromě této složky `Složka` samotné. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.
    - Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.
11. V bloku **Součásti ochrany** vyberte součást **Detekce chování**.
12. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

13. Vyberte pro výjimku stav **Aktivní**.

    Pomocí přepínače můžete výjimku kdykoli ukončit.

14. Uložte změny.

Jak vytvořit výjimku pro ochranu sdílených složek v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecné nastavení** → **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.
4. Klikněte na tlačítko **Přidat**.
5. Klikněte na tlačítko **Procházet** a vyberte sdílenou složku.

   Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`:

   - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
   - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Složka` kromě této složky `Složka` samotné. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.
   - Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.

6. V bloku **Součásti ochrany** vyberte součást **Detekce chování**.
7. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.
8. Vyberte pro výjimku stav **Aktivní**.

   Pomocí přepínače můžete výjimku kdykoli ukončit.

9. Uložte změny.

Konfigurace adres výjimek z ochrany sdílených složek proti externímu šifrování

Aby bylo možné povolit výjimky adres z ochrany sdílených složek proti externímu šifrování, je nutné povolit funkci auditování přihlášení. Ve výchozím nastavení je služba auditování přihlášení zakázaná (podrobné informace o povolení služby auditování přihlášení najdete na webu společnosti Microsoft).

Funkce vyloučení adres z ochrany sdílených složek nefunguje ve vzdáleném počítači, pokud byl vzdálený počítač zapnut před spuštěním aplikace Kaspersky Endpoint Security. Po spuštění aplikace Kaspersky Endpoint Security můžete tento vzdálený počítač restartovat, čímž zajistíte, že funkce vyloučení adres z ochrany sdílených složek bude v tomto vzdáleném počítači fungovat.

Postup vyloučení vzdálených počítačů provádějících externí šifrování sdílených složek:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Detekce chování**.
3. V bloku **Výjimky** klikněte na odkaz **Nakonfigurujte adresy výjimek**.
4. Pokud chcete přidat IP adresu nebo název počítače do seznamu výjimek, klikněte na tlačítko **Přidat**.
5. Zadejte IP adresu nebo název počítače, ze kterých nesmí být zpracovány pokusy o externí šifrování.
6. Uložte změny.

Export a import seznamu výjimek z ochrany sdílených složek před externím šifrováním

Seznam výjimek můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství adres stejného typu. Funkci exportu/importu můžete také použít k zálohování seznamu výjimek nebo k migraci seznamu na jiný server.

Jak exportovat a importovat seznam výjimek v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Detekce chování**.
6. V oddílu **Ochrana sdílených složek proti externímu šifrování** klikněte na tlačítko **Výjimky**.
7. Postup exportu seznamu pravidel:
   a. Vyberte výjimky, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádnou výjimku nevybrali, aplikace Kaspersky Endpoint Security exportuje všechny výjimky.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
8. Postup importu seznamu výjimek:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
9. Uložte změny.

[Jak exportovat a importovat seznam výjimek ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam výjimek.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnost **Rozšířená ochrana před hrozbami** → **Detekce chování**.
5. Postup exportu seznamu výjimek v bloku **Výjimky**:
   a. Vyberte výjimky, které chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrďte, jestli chcete exportovat pouze vybrané výjimky, nebo exportovat celý seznam výjimek.
   d. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   e. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
6. Postup importu seznamu výjimek v bloku **Výjimky**:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
7. Uložte změny.

Prevence narušení hostitele

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Prevence narušení hostitele zabraňuje aplikacím provádět akce, které mohou být pro operační systém nebezpečné, a kontroluje přístup k prostředkům operačního systému a osobním datům. Tato součást poskytuje ochranu počítače pomocí antivirových databází a cloudové služby Kaspersky Security Network.

Součást řídí provoz aplikací pomocí *oprávnění aplikací*. Oprávnění aplikací zahrnují následující parametry přístupu:

- Přístup k prostředkům operačního systému (například možnosti automatického spuštění, klíče registru)

- Přístup k osobním datům (jako jsou soubory a aplikace)

Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.

Během prvního spuštění aplikace provádí součást Prevence narušení hostitele následující akce:

1. Zkontroluje zabezpečení aplikace pomocí stažených antivirových databází.
2. Zkontroluje zabezpečení webu ve službě Kaspersky Security Network.

   Doporučujeme vám zapojit se do služby Kaspersky Security Network, čímž nám pomůžete zajistit účinnější fungování součásti Prevence narušení hostitele.

3. Umístí aplikaci do jedné ze *skupin důvěryhodnosti*: Důvěryhodné, Nízké omezení, Vysoké omezení, Nedůvěryhodné.

   Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace. Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat.

   Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti pro součásti Brána firewall a Prevence narušení hostitele. Skupinu důvěryhodnosti nelze změnit pouze u součástí Brána firewall a Prevence narušení hostitele.

   Pokud jste účast v KSN odmítli nebo neexistuje žádná síť, aplikace Kaspersky Endpoint Security umístí aplikaci do skupiny důvěryhodnosti v závislosti na nastavení součásti Prevence narušení hostitele. Po obdržení reputace aplikace z KSN lze skupinu důvěryhodnosti změnit automaticky.

4. Blokuje akce aplikace v závislosti na skupině důvěryhodnosti. Například aplikacím ze skupiny důvěryhodných s omezeným přístupem je odepřen přístup k modulům operačního systému.

Při příštím spuštění aplikace ověří součást aplikace Kaspersky Endpoint Security integritu aplikace. Pokud je aplikace nezměněná, součást pro ni použije aktuální oprávnění aplikací. Pokud došlo ke změně aplikace, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spouštěna poprvé.

Povolení a zakázání součásti Prevence narušení hostitele

Ve výchozím nastavení je součást Prevence narušení hostitele povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky.

Jak povolit nebo zakázat součást Prevence narušení hostitele v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
6. Pomocí zaškrtávacího políčka **Prevence narušení hostitele** můžete tuto součást povolit nebo zakázat.
7. Uložte změny.

Jak povolit nebo zakázat součást Prevence narušení hostitele ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení → Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
5. Pomocí přepínače **Prevence narušení hostitele** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

Jak povolit nebo zakázat součást Prevence narušení hostitele v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
3. Pomocí přepínače **Prevence narušení hostitele** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Je-li součást Prevence narušení hostitele povolena, aplikace Kaspersky Endpoint Security umístí aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat. Aplikace Kaspersky Endpoint Security poté zablokuje akce aplikace v závislosti na skupině důvěryhodnosti.

Správa skupin důvěryhodnosti aplikací

Při prvním spuštění každé aplikace zkontroluje součást Prevence narušení hostitele zabezpečení aplikace a umístí ji do některé ze skupin důvěryhodnosti.

V první fázi kontroly aplikace se aplikace Kaspersky Endpoint Security pokusí najít odpovídající záznam v interní databázi známých aplikací a současně vyšle požadavek do databáze Kaspersky Security Network (pokud je k dispozici připojení k internetu). Na základě výsledků vyhledávání v interní databázi a databázi Kaspersky Security Network bude aplikace umístěna do skupiny důvěryhodnosti. Při každém následném spuštění aplikace vyšle aplikace Kaspersky Endpoint Security nový dotaz do databáze služby KSN a umístí aplikaci do jiné skupiny důvěryhodnosti, pokud se důvěryhodnost aplikace v databázi služby KSN změnila.

Můžete vybrat skupinu důvěryhodnosti, do které musí aplikace Kaspersky Endpoint Security automaticky zařadit všechny neznámé aplikace. Aplikace, které byly spuštěny před aplikací Kaspersky Endpoint Security, jsou automaticky přesunuty do skupiny důvěryhodnosti definované v okně nastavení součásti Prevence narušení hostitele.

V případě aplikací, které byly spuštěny před aplikací Kaspersky Endpoint Security, je kontrolována pouze síťová aktivita. Kontrola je prováděna v souladu s pravidly sítě definovaným v nastavení brány firewall.

Změna skupiny důvěryhodnosti aplikace

Při prvním spuštění každé aplikace zkontroluje součást Prevence narušení hostitele zabezpečení aplikace a umístí ji do některé ze skupin důvěryhodnosti.

Odborníci společnosti Kaspersky nedoporučují přesouvání aplikací z automaticky přiřazené skupiny důvěryhodnosti do jiné skupiny důvěryhodnosti. Místo toho můžete v případě potřeby upravit oprávnění pro jednotlivou aplikaci.

Jak změnit skupinu důvěryhodnosti aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **Oprávnění aplikací** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
7. Vyberte kartu **Oprávnění aplikací**.
8. Klikněte na tlačítko **Přidat**.
9. V okně, které se otevře, zadejte kritéria pro vyhledání aplikace, jejíž skupinu důvěryhodnosti chcete změnit.

   Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
10. Klikněte na tlačítko **Aktualizovat**.

    Aplikace Kaspersky Endpoint Security vyhledá aplikaci v konsolidovaném seznamu aplikací nainstalovaných na spravovaných počítačích. Aplikace Kaspersky Endpoint Security zobrazí seznam aplikací, které splňují vaše vyhledávací kritéria.
11. Vyberte požadovanou aplikaci.
12. V rozevíracím seznamu **Přidat vybrané aplikace do <skupina zabezpečení>** vyberte požadovanou skupinu důvěryhodnosti pro aplikaci.
13. Uložte změny.

Jak změnit skupinu důvěryhodnosti aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na odkaz **Oprávnění aplikace a chráněné prostředky**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Vyberte kartu **Oprávnění aplikací**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.
7. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.
8. Klikněte na odkaz **Vybraná cílová skupina** a vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.
9. Vyberte typ **Aplikace**. Klikněte na tlačítko **Další**.

   Pokud chcete změnit skupinu důvěryhodnosti pro více aplikací, vyberte typ **Skupina** a definujte název skupiny aplikací.
10. V seznamu aplikací, který se otevře, vyberte aplikace, jejichž skupinu důvěryhodnosti chcete změnit.

    Použijte filtr. Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
11. Dokončete průvodce kliknutím na tlačítko **OK**.

    Aplikace bude přidána do skupiny důvěryhodnosti.
12. Uložte změny.

[Jak změnit skupinu důvěryhodnosti aplikace v rozhraní aplikace]

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. Klikněte na tlačítko **Správa aplikací**.

   Otevře se seznam nainstalovaných aplikací.
4. Vyberte požadovanou aplikaci.
5. V místní nabídce aplikace vyberte možnost **Omezení** → <σκυπινα δůϖěρψηοδνοστι>.
6. Uložte změny.

Aplikace tak bude vložena do jiné skupiny důvěryhodností. Aplikace Kaspersky Endpoint Security poté zablokuje akce aplikace v závislosti na skupině důvěryhodnosti. Aplikaci bude přiřazen stav *(definovaný uživatelem)*. Pokud se v aplikaci Kaspersky Security Network změní pověst aplikace, součást Prevence narušení hostitele ponechá skupinu důvěryhodnosti této aplikace beze změny.

Konfigurace práv skupiny důvěryhodnosti

Ve výchozím nastavení jsou vytvořena pro různé skupiny důvěryhodnosti optimální práva aplikace. Nastavení oprávnění skupin aplikací, které jsou ve skupině důvěryhodnosti, dědí hodnoty z nastavení oprávnění skupiny důvěryhodnosti.

Jak změnit práva skupiny důvěryhodnosti v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **Oprávnění aplikací** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
7. Vyberte kartu **Oprávnění aplikací**.
8. Vyberte příslušnou skupinu důvěryhodnosti.
9. V místní nabídce skupiny důvěryhodností vyberte možnost **Oprávnění skupin**.

   Tím otevřete vlastnosti skupiny důvěryhodnosti.
10. Proveďte jednu z následujících akcí:

    - Chcete-li upravit oprávnění skupin důvěryhodnosti, která řídí operace s registrem operačního systému, uživatelským souborům a nastavením aplikací, vyberte kartu **Soubory a systémový registr**.
    - Pokud chcete upravit oprávnění skupin důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte kartu **Práva**.

    Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.
11. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši a otevřete místní nabídku a vyberte potřebnou možnost: **Dědit**, **Povolit** (✓) nebo **Zakázat** (⊘).
12. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapsat do zprávy** (✓/⊘).

    Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.
13. Uložte změny.

Jak změnit oprávnění skupiny důvěryhodnosti ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na odkaz **Oprávnění aplikace a chráněné prostředky**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Vyberte kartu **Oprávnění aplikací**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.
7. V levé části okna vyberte příslušnou skupinu důvěryhodnosti.
8. V pravé části okna v rozevíracím seznamu proveďte jednu z následujících akcí:

   - Pokud chcete upravit oprávnění skupiny důvěryhodnosti, která regulují operace s registrem operačního systému, uživatelskými soubory a nastavením aplikace, vyberte možnost **Soubory a systémový registr**.
   - Jestliže chcete upravit oprávnění skupiny důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte možnost **Práva**.

   Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.
9. U příslušného zdroje ve sloupci odpovídající akce vyberte požadovanou možnost: **Dědit**, **Povolit** (✓) nebo **Zakázat** (✗).
10. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapsat do zprávy** (✓/✗).

    Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.
11. Uložte změny.

Jak změnit oprávnění skupiny důvěryhodností v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. Klikněte na tlačítko **Správa aplikací**.

   Otevře se seznam nainstalovaných aplikací.
4. Vyberte příslušnou skupinu důvěryhodnosti.
5. V místní nabídce skupiny důvěryhodnosti vyberte možnost **Podrobnosti a pravidla**.

   Tím otevřete vlastnosti skupiny důvěryhodnosti.
6. Proveďte jednu z následujících akcí:
   - Chcete-li upravit oprávnění skupin důvěryhodnosti, která řídí operace s registrem operačního systému, uživatelským souborům a nastavením aplikací, vyberte kartu **Soubory a systémový registr**.
   - Pokud chcete upravit oprávnění skupin důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte kartu **Práva**.

   Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.
7. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši, otevřete místní nabídku a vyberte požadovanou možnost: **Dědit**, **Povolit** () nebo **Zakázat** ().
8. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapisovat do zprávy** ().

   Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.
9. Uložte změny.

Oprávnění skupiny důvěryhodnosti budou změněna. Aplikace Kaspersky Endpoint Security poté zablokuje akce aplikace v závislosti na skupině důvěryhodnosti. Skupině důvěryhodnosti bude přiřazen stav (*uživatelské nastavení*).

Výběr skupiny důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security

V případě aplikací, které byly spuštěny před aplikací Kaspersky Endpoint Security, je kontrolována pouze síťová aktivita. Kontrola je prováděna v souladu s pravidly sítě definovanými v nastavení brány firewall. Chcete-li určit, která pravidla sítě mají být použita na monitorování síťové aktivity pro tyto aplikace, musíte zvolit skupinu důvěryhodnosti.

Jak vybrat skupinu důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
6. V části **Oprávnění aplikací** klikněte na tlačítko **Upravit**.
7. Vyberte příslušnou skupinu důvěryhodnosti pro nastavení **Aplikace spuštěné před aplikací Kaspersky Endpoint Security pro systém Windows jsou automaticky přesunuty do skupiny důvěryhodnosti <skupina důvěryhodnosti>**.
8. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení → Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
5. Vyberte příslušnou skupinu důvěryhodnosti pro nastavení **Aplikace spuštěné před aplikací Kaspersky Endpoint Security pro systém Windows jsou automaticky přesunuty do skupiny důvěryhodnosti <skupina důvěryhodnosti>**.
6. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. Vyberte příslušnou skupinu důvěryhodnosti v nastavení **Aplikace spuštěné před aplikací Kaspersky Endpoint Security pro systém Windows jsou automaticky přesunuty do skupiny důvěryhodnosti <skupina důvěryhodnosti>**.
4. Uložte změny.

Aplikace spuštěná před aplikací Kaspersky Endpoint Security tak bude zařazena do jiné skupiny důvěryhodnosti. Aplikace Kaspersky Endpoint Security poté zablokuje akce aplikace v závislosti na skupině důvěryhodnosti.

Výběr skupiny důvěryhodnosti pro neznámé aplikace

Během prvního spuštění aplikace určuje součást Prevence narušení hostitele skupinu důvěryhodnosti aplikace. Pokud nemáte přístup k internetu nebo pokud služba Kaspersky Security Network nemá o této aplikaci žádné informace, aplikace Kaspersky Endpoint Security ve výchozím nastavení umístí aplikaci do skupiny s nízkým omezením. Pokud jsou v KSN zjištěny informace o dříve neznámé aplikaci, aplikace Kaspersky Endpoint Security aktualizuje práva této aplikace. Poté můžete oprávnění aplikací ručně upravit.

Jak vybrat skupinu důvěryhodnosti pro neznámé aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **pravidel pro zpracování aplikací** pomocí rozevíracího seznamu **Skupina důvěryhodnosti pro aplikace, které nelze přiřadit k jiným skupinám** vyberte požadovanou skupinu důvěryhodnosti.

   Pokud je povolena účast ve službě Kaspersky Security Network, aplikace Kaspersky Endpoint Security odešle do služby KSN požadavek ohledně reputace aplikace při každém spuštění aplikace. Na základě obdržené odpovědi může být aplikace přesunuta do jiné skupiny důvěryhodnosti, než jaká je určena v nastavení součásti Prevence narušení hostitele.
7. Pomocí zaškrtávacího políčka **Aktualizovat práva pro dříve neznámé aplikace z databáze služby KSN** nakonfigurujte automatickou aktualizaci oprávnění neznámých aplikací.
8. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro neznámé aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **pravidel pro zpracování aplikací** pomocí rozevíracího seznamu **Skupina důvěryhodnosti pro aplikace, které nelze přiřadit k jiným skupinám** vyberte požadovanou skupinu důvěryhodnosti.

   Pokud je povolena účast ve službě Kaspersky Security Network, aplikace Kaspersky Endpoint Security odešle do služby KSN požadavek ohledně reputace aplikace při každém spuštění aplikace. Na základě obdržené odpovědi může být aplikace přesunuta do jiné skupiny důvěryhodnosti, než jaká je určena v nastavení součásti Prevence narušení hostitele.
6. Pomocí zaškrtávacího políčka **Aktualizovat práva pro dříve neznámé aplikace z databáze služby KSN** nakonfigurujte automatickou aktualizaci oprávnění neznámých aplikací.
7. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro neznámé aplikace v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Skupina důvěryhodnosti pro neznámé aplikace** vyberte příslušnou skupinu důvěryhodnosti.

   Pokud je povolena účast ve službě Kaspersky Security Network, aplikace Kaspersky Endpoint Security odešle do služby KSN požadavek ohledně reputace aplikace při každém spuštění aplikace. Na základě obdržené odpovědi může být aplikace přesunuta do jiné skupiny důvěryhodnosti, než jaká je určena v nastavení součásti Prevence narušení hostitele.
4. Pomocí zaškrtávacího políčka **Aktualizovat práva pro dříve neznámé aplikace z databáze služby KSN** nakonfigurujte automatickou aktualizaci oprávnění neznámých aplikací.
5. Uložte změny.

Výběr skupiny důvěryhodnosti pro digitálně podepsané aplikace

Aplikace Kaspersky Endpoint Security vždy umístí aplikace podepsané certifikáty společnosti Microsoft nebo certifikáty společnosti Kaspersky do skupiny Důvěryhodné.

Jak vybrat skupinu důvěryhodnosti pro digitálně podepsané aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
6. V bloku **Pravidla zpracování aplikací** pomocí zaškrtávacího políčka **Důvěřovat aplikacím s digitálním podpisem** povolte nebo zakažte automatické přiřazení skupině Důvěryhodné pro aplikace obsahující digitální podpis důvěryhodných vydavatelů.

   Důvěryhodní dodavatelé jsou ti dodavatelé softwaru, které společnost Kaspersky zařadila do skupiny důvěryhodnosti. Certifikát dodavatele můžete také přidat do úložiště důvěryhodných systémových certifikátů ručně.

   Jestliže je zaškrtnutí tohoto políčka zrušeno, nebude součást Prevence narušení hostitele považovat digitálně podepsané aplikace za důvěryhodné a použije k určení jejich skupiny důvěryhodnosti jiné parametry.
7. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro digitálně podepsané aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení → Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
5. V bloku **Pravidla zpracování aplikací** pomocí zaškrtávacího políčka **Důvěřovat aplikacím s digitálním podpisem** povolte nebo zakažte automatické přiřazení skupině Důvěryhodné pro aplikace obsahující digitální podpis důvěryhodných vydavatelů.

   Důvěryhodní dodavatelé jsou ti dodavatelé softwaru, které společnost Kaspersky zařadila do skupiny důvěryhodnosti. Certifikát dodavatele můžete také přidat do úložiště důvěryhodných systémových certifikátů ručně.

   Jestliže je zaškrtnutí tohoto políčka zrušeno, nebude součást Prevence narušení hostitele považovat digitálně podepsané aplikace za důvěryhodné a použije k určení jejich skupiny důvěryhodnosti jiné parametry.
6. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro digitálně podepsané aplikace v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Pravidla zpracování aplikací** pomocí zaškrtávacího políčka **Důvěřovat aplikacím s digitálním podpisem** povolte nebo zakažte automatické přiřazení skupině Důvěryhodné pro aplikace obsahující digitální podpis důvěryhodných vydavatelů.

   Důvěryhodní dodavatelé jsou ti dodavatelé softwaru, které společnost Kaspersky zařadila do skupiny důvěryhodnosti. Certifikát dodavatele můžete také přidat do úložiště důvěryhodných systémových certifikátů ručně.

   Jestliže je zaškrtnutí tohoto políčka zrušeno, nebude součást Prevence narušení hostitele považovat digitálně podepsané aplikace za důvěryhodné a použije k určení jejich skupiny důvěryhodnosti jiné parametry.
4. Uložte změny.

Konfigurace oprávnění aplikací

Ve výchozím nastavení je aktivita aplikace řízena na základě práv aplikace definovaných pro konkrétní skupinu důvěryhodnosti, kterou aplikace Kaspersky Endpoint Security přiřadila aplikaci při jejím prvním spuštění. Pokud je to nutné, můžete oprávnění aplikací upravit pro celou skupinu důvěryhodnosti, pro jednotlivou aplikaci nebo pro skupinu aplikací v rámci skupiny důvěryhodnosti.

Ručně definovaná oprávnění aplikací mají vyšší prioritu než oprávnění aplikací, která byla definována pro skupinu důvěryhodnosti. Jinými slovy, pokud se ručně definovaná oprávnění aplikací liší od oprávnění aplikací definovaných pro skupinu důvěryhodnosti, součást Prevence narušení hostitele řídí činnost aplikace podle ručně definovaných oprávnění aplikací.

Pravidla, která vytvoříte pro aplikace, jsou zděděna podřízenými aplikacemi. Například pokud odmítnete veškerou síťovou aktivitu pro cmd.exe, veškerá síťová aktivita bude také odepřena pro notepad.exe, pokud je spuštěn pomocí cmd.exe. Pokud je aplikace spuštěna nepřímo jinou aplikací, ale není podřízenou aplikací, ze které běží, pravidla se nezdědí.

Jak změnit oprávnění aplikací v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **Oprávnění aplikací** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
7. Vyberte kartu **Oprávnění aplikací**.
8. Klikněte na tlačítko **Přidat**.
9. V okně, které se otevře, zadejte kritéria pro vyhledání aplikace, jejíž práva chcete změnit.

   Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
10. Klikněte na tlačítko **Aktualizovat**.

    Aplikace Kaspersky Endpoint Security vyhledá aplikaci v konsolidovaném seznamu aplikací nainstalovaných na spravovaných počítačích. Aplikace Kaspersky Endpoint Security zobrazí seznam aplikací, které splňují vaše vyhledávací kritéria.
11. Vyberte požadovanou aplikaci.
12. V rozevíracím seznamu **Přidat vybrané aplikace do <skupina zabezpečení>** Rozevírací vyberte položku **Výchozí skupiny** a klikněte na tlačítko **OK**.

    Aplikace bude přidána do výchozí skupiny.
13. Vyberte příslušnou aplikaci a poté vyberte možnost **Oprávnění aplikací** v místní nabídce aplikace.

    Otevřou se vlastnosti aplikace.
14. Proveďte jednu z následujících akcí:

    - Chcete-li upravit oprávnění skupin důvěryhodnosti, která řídí operace s registrem operačního systému, uživatelským souborům a nastavením aplikací, vyberte kartu **Soubory a systémový registr**.
    - Pokud chcete upravit oprávnění skupin důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte kartu **Práva**.

    Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.
15. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši a otevřete místní nabídku a vyberte potřebnou možnost: **Dědit**, **Povolit** (✓) nebo **Zakázat** (⊘).
16. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapsat do zprávy** (✓/⊘).

Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.

17. Uložte změny.

[Jak změnit oprávnění aplikací ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na odkaz **Oprávnění aplikace a chráněné prostředky**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Vyberte kartu **Oprávnění aplikací**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.
7. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.
8. Klikněte na odkaz **Vybraná cílová skupina** a vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.
9. Vyberte typ **Aplikace**. Klikněte na tlačítko **Další**.

   Pokud chcete změnit skupinu důvěryhodnosti pro více aplikací, vyberte typ **Skupina** a definujte název skupiny aplikací.
10. V seznamu aplikací, který se otevře, vyberte aplikace, jejichž oprávnění chcete změnit.

    Použijte filtr. Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
11. Dokončete průvodce kliknutím na tlačítko **OK**.

    Aplikace bude přidána do skupiny důvěryhodnosti.
12. V levé části okna vyberte příslušnou aplikaci.
13. V pravé části okna v rozevíracím seznamu proveďte jednu z následujících akcí:

    - Pokud chcete upravit oprávnění skupiny důvěryhodnosti, která regulují operace s registrem operačního systému, uživatelskými soubory a nastavením aplikace, vyberte možnost **Soubory a systémový registr**.
    - Jestliže chcete upravit oprávnění skupiny důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte možnost **Práva**.

    Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.
14. U příslušného zdroje ve sloupci odpovídající akce vyberte požadovanou možnost: **Dědit**, **Povolit** (✓) nebo **Zakázat** (✗).
15. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapsat do zprávy** (✓/✗).

Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.

16. Uložte změny.

[Jak změnit oprávnění aplikací v rozhraní aplikace](#)

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. Klikněte na tlačítko **Správa aplikací**.

   Otevře se seznam nainstalovaných aplikací.
4. Vyberte požadovanou aplikaci.
5. V kontextové nabídce aplikace vyberte možnost **Podrobnosti a pravidla**.

   Otevřou se vlastnosti aplikace.
6. Proveďte jednu z následujících akcí:

   - Chcete-li upravit oprávnění skupin důvěryhodnosti, která řídí operace s registrem operačního systému, uživatelským souborům a nastavením aplikací, vyberte kartu **Soubory a systémový registr**.
   - Pokud chcete upravit oprávnění skupin důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte kartu **Práva**.
7. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši, otevřete místní nabídku a vyberte požadovanou možnost: **Dědit**, **Povolit** () nebo **Zakázat** ().
8. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Zapisovat do zprávy** ().

   Aplikace Kaspersky Endpoint Security bude zaznamenávat informace o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.
9. Vyberte kartu **Výjimky** a nakonfigurujte rozšířené nastavení aplikace (viz tabulka níže).
10. Uložte změny.

Rozšířené nastavení aplikace

Parametr	Popis
Nekontrolovat otevírané soubory	Z kontroly aplikací Kaspersky Endpoint Security jsou vyloučeny všechny soubory, které otevírá tato aplikace. Pokud například používáte aplikace k zálohování souborů, tato funkce pomáhá snížit spotřebu prostředků aplikací Kaspersky Endpoint Security.
Nesledovat činnost aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat souborovou ani síťovou aktivitu aplikace v operačním systému. Činnost aplikace je monitorována následujícími součástmi: Detekce chování, Prevence zneužití, Prevence narušení hostitele, Nástroj pro nápravu a Brána firewall.
Nedědit omezení nadřazeného procesu (aplikace)	Omezení nakonfigurovaná pro nadřazený proces nebude aplikace Kaspersky Endpoint Security používat na podřízený proces. Nadřazený proces je spuštěn aplikací, pro kterou jsou nakonfigurována práva aplikace (Prevence narušení hostitele) a pravidla sítě aplikace (Brána firewall).
Nesledovat činnost podřízených aplikací	Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu souborů ani síťovou aktivitu aplikací spuštěných touto aplikací.

Povolit interakci s rozhraním aplikace Kaspersky Endpoint Security	Sebeobrana aplikace Kaspersky Endpoint Security blokuje všechny pokusy o správu služeb aplikace ze vzdáleného počítače. Je-li políčko vybráno, je aplikaci se vzdáleným přístupem povoleno spravovat nastavení aplikace Kaspersky Endpoint Security prostřednictvím rozhraní aplikace Kaspersky Endpoint Security.
Nekontrolovat šifrovaný provoz / **Nekontrolovat veškerý provoz**	Síťový provoz iniciovaný touto aplikací bude vyloučen z kontroly aplikací Kaspersky Endpoint Security. Z kontroly můžete vyloučit buď veškerý provoz, nebo pouze šifrovaný provoz. Z kontroly můžete také vyloučit jednotlivé adresy IP a čísla portů.

Ochrana prostředků operačního systému a osobních údajů

Součást Prevence narušení hostitele spravuje oprávnění aplikací za účelem vykonávání akcí v souvislosti s různými kategoriemi prostředků operačního systému a osobních dat. Odborníci společnosti Kaspersky vytvořili přednastavené kategorie chráněných prostředků. Například kategorie *Operační systém* má podkategorii *Nastavení spuštění*, která uvádí všechny klíče registru spojené s automatickým spuštěním aplikací. Přednastavené kategorie chráněných prostředků ani chráněné prostředky v rámci těchto kategorií nemůžete upravit ani odstranit.

Jak přidat chráněný prostředek v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **Oprávnění aplikací** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
7. Vyberte kartu **Chráněné prostředky**.

   V levé části okna se zobrazí seznam chráněných prostředků a odpovídající oprávnění pro přístup k těmto prostředkům v závislosti na konkrétní skupině důvěryhodnosti.
8. Vyberte kategorii chráněných prostředků, do nichž chcete přidat nový chráněný prostředek.

   Chcete-li přidat podkategorii, klikněte na položky **Přidat** → **Kategorie**.
9. Klikněte na tlačítko **Přidat**. V rozevíracím seznamu vyberte typ prostředku, který chcete přidat: **Soubor nebo složka** nebo **Klíč registru**.
10. V okně, které se otevře, vyberte soubor, složku nebo klíč registru.

    Můžete zobrazit oprávnění aplikací pro přístup k přidaným prostředkům. Chcete-li tak učinit, vyberte v levé části okna přidaný prostředek a aplikace Kaspersky Endpoint Security zobrazí přístupová oprávnění pro každou skupinu důvěryhodnosti. Můžete také zakázat řízení aktivity aplikace s prostředky pomocí zaškrtávacího políčka vedle nového prostředku.
11. Uložte změny.

Jak přidat chráněný prostředek ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na odkaz **Oprávnění aplikace a chráněné prostředky**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Vyberte kartu **Chráněné prostředky**.

   V levé části okna se zobrazí seznam chráněných prostředků a odpovídající oprávnění pro přístup k těmto prostředkům v závislosti na konkrétní skupině důvěryhodnosti.
7. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce novým prostředkem.
8. Klikněte na odkaz **Název skupiny** a vyberte kategorii chráněných prostředků, do nichž chcete přidat nový chráněný prostředek.

   Pokud chcete přidat podkategorii, vyberte možnost **Kategorie chráněných prostředků**.
9. Vyberte typ prostředku, který chcete přidat: **Soubor nebo složka** nebo **Klíč registru**.
10. Vyberte soubor, složku nebo klíč registru.
11. Dokončete průvodce kliknutím na tlačítko **OK**.

    Můžete zobrazit oprávnění aplikací pro přístup k přidaným prostředkům. Chcete-li tak učinit, vyberte v levé části okna přidaný prostředek a aplikace Kaspersky Endpoint Security zobrazí přístupová oprávnění pro každou skupinu důvěryhodnosti. Můžete také použít zaškrtávací políčko ve sloupci **Stav** a deaktivovat řízení aktivity aplikace s prostředky.
12. Uložte změny.

Jak přidat chráněný prostředek v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. Klikněte na tlačítko **Správa prostředků**.

   Otevře se seznam chráněných prostředků.
4. Vyberte kategorii chráněných prostředků, do nichž chcete přidat nový chráněný prostředek.

   Chcete-li přidat podkategorii, klikněte na položky **Přidat** → **Kategorie**.
5. Klikněte na tlačítko **Přidat**. V rozevíracím seznamu vyberte typ prostředku, který chcete přidat: **Soubor nebo složka** nebo **Klíč registru**.
6. V okně, které se otevře, vyberte soubor, složku nebo klíč registru.

   Můžete zobrazit oprávnění aplikací pro přístup k přidaným prostředkům. Chcete-li tak učinit, vyberte v levé části okna přidaný prostředek a aplikace Kaspersky Endpoint Security zobrazí seznam aplikací a přístupová práva pro jednotlivé aplikace. Můžete také zakázat kontrolu aktivity aplikace s prostředky pomocí tlačítka **Zakázat kontrolu** ve sloupci **Stav**.
7. Uložte změny.

Kaspersky Endpoint Security bude řídit přístup k přidaným prostředkům operačního systému a k osobním údajům. Kaspersky Endpoint Security řídí přístup aplikace k prostředkům na základě skupiny důvěryhodnosti přiřazené aplikaci. Skupinu důvěryhodnosti aplikace můžete také změnit.

Odstraňování informací o nepoužívaných aplikacích

Aplikace Kaspersky Endpoint Security používá k řízení činností aplikací oprávnění aplikací. Oprávnění aplikací jsou určena jejich skupinou důvěryhodnosti. Při prvním spuštění aplikace Kaspersky Endpoint Security zařadí aplikaci do skupiny důvěryhodných. Skupinu důvěryhodnosti aplikace můžete ručně změnit. Oprávnění jednotlivých aplikací můžete také ručně nakonfigurovat. Aplikace Kaspersky Endpoint Security ukládá následující informace o aplikaci: skupina důvěryhodnosti aplikace a oprávnění aplikace.

Aplikace Kaspersky Endpoint Security automaticky odstraňuje informace o nepoužitých aplikacích a šetří tak prostředky počítače. Aplikace Kaspersky Endpoint Security odstraňuje informace o aplikaci podle následujících pravidel:

- Pokud byly skupina důvěryhodnosti a oprávnění aplikace stanoveny automaticky, aplikace Kaspersky Endpoint Security odstraní informace o této aplikaci po 30 dnech. Není možné změnit dobu uložení informací o aplikaci ani vypnout automatické odstranění.
- Pokud aplikaci do skupiny důvěryhodnosti zařadíte ručně nebo nakonfigurujete její přístupová práva, aplikace Kaspersky Endpoint Security odstraní informace o této aplikaci po 60 dnech (výchozí doba uložení). Můžete změnit dobu uložení informací o aplikaci nebo vypnout automatické odstranění (viz pokyny níže).

Při spuštění aplikace, jejíž informace byly odstraněny, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spuštěna poprvé.

Jak nakonfigurovat automatické odstraňování informací o nepoužívaných aplikacích v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
6. V bloku **Pravidla zpracování aplikací** proveďte jednu z následujících akcí:
   - Pokud chcete nakonfigurovat automatické odstraňování, zaškrtněte políčko **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** a zadejte požadovaný počet dní.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, aplikace Kaspersky Endpoint Security za určitý počet dní odstraní. Aplikace Kaspersky Endpoint Security po 30 dnech také odstraní informace o aplikacích, jejichž skupina důvěry a práva na aplikace byla stanovena automaticky.
   - Pokud chcete automatické odstraňování vypnout, zaškrtnutí políčka **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** zrušte.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, bude aplikace Kaspersky Endpoint Security ukládat na dobu neurčitou bez jakéhokoli omezení doby uložení. Aplikace Kaspersky Endpoint Security bude odstraňovat pouze informace o aplikacích, jejichž skupina důvěryhodnosti a oprávnění aplikací byly určeny automaticky po 30 dnech.
7. Uložte změny.

[Jak nakonfigurovat automatické odstraňování informací o nepoužívaných aplikacích ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
5. V bloku **Pravidla zpracování aplikací** proveďte jednu z následujících akcí:

   - Pokud chcete nakonfigurovat automatické odstraňování, zaškrtněte políčko **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** a zadejte požadovaný počet dní.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, aplikace Kaspersky Endpoint Security za určitý počet dní odstraní. Aplikace Kaspersky Endpoint Security po 30 dnech také odstraní informace o aplikacích, jejichž skupina důvěry a práva na aplikace byla stanovena automaticky.

   - Pokud chcete automatické odstraňování vypnout, zaškrtnutí políčka **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** zrušte.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, bude aplikace Kaspersky Endpoint Security ukládat na dobu neurčitou bez jakéhokoli omezení doby uložení. Aplikace Kaspersky Endpoint Security bude odstraňovat pouze informace o aplikacích, jejichž skupina důvěryhodnosti a oprávnění aplikací byly určeny automaticky po 30 dnech.
6. Uložte změny.

Jak nakonfigurovat automatické odstraňování informací o nepoužívaných aplikacích v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Pravidla zpracování aplikací** proveďte jednu z následujících akcí:
   - Pokud chcete nakonfigurovat automatické odstraňování, zaškrtněte políčko **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** a zadejte požadovaný počet dní.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, aplikace Kaspersky Endpoint Security za určitý počet dní odstraní. Aplikace Kaspersky Endpoint Security po 30 dnech také odstraní informace o aplikacích, jejichž skupina důvěry a práva na aplikace byla stanovena automaticky.
   - Pokud chcete automatické odstraňování vypnout, zaškrtnutí políčka **Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní** zrušte.

     Informace o aplikacích, které ručně vložíte do skupiny důvěryhodnosti nebo jejichž přístupová práva jste ručně nakonfigurovali, bude aplikace Kaspersky Endpoint Security ukládat na dobu neurčitou bez jakéhokoli omezení doby uložení. Aplikace Kaspersky Endpoint Security bude odstraňovat pouze informace o aplikacích, jejichž skupina důvěryhodnosti a oprávnění aplikací byly určeny automaticky po 30 dnech.
4. Uložte změny.

Sledování součásti Prevence narušení hostitele

Můžete přijímat zprávy o fungování součásti Prevence narušení hostitele. Zprávy obsahují informace o operacích s počítačovými prostředky prováděných aplikací (povolené nebo zakázané). Zprávy také obsahují informace o aplikacích, které využívají jednotlivé prostředky.

Chcete-li sledovat operace součásti Prevence narušení hostitele, musíte povolit zápis zpráv. Můžete například povolit přeposílání zpráv pro jednotlivé aplikace v nastavení součásti Prevence narušení hostitele.

Při konfiguraci sledování součásti Prevence narušení hostitele berte v úvahu potenciální zatížení sítě při předávání událostí do aplikace Kaspersky Security Center. Ukládání zpráv můžete také povolit pouze v místním protokolu aplikace Kaspersky Endpoint Security.

Ochrana přístupu ke zvuku a videu

Počítačoví zločinci se mohou pomocí speciálních programů pokusit získat přístup k zařízením, která zaznamenávají zvuk a video (například mikrofony nebo webové kamery). Kaspersky Endpoint Security kontroluje, kdy aplikace přijímají datový proud zvuku nebo videa, a chrání data před neoprávněným zachycením.

Ve výchozím nastavení Kaspersky Endpoint Security kontroluje přístup aplikací k datovému proudu zvuku nebo videa na základě kategorie aplikace:

- Důvěryhodné aplikace a aplikace s nízkým omezením mají ve výchozím nastavení povoleno přijímat datový proud zvuku a videa ze zařízení.
- Aplikace s vysokým omezením a nedůvěryhodné aplikace nemají ve výchozím nastavení povoleno přijímat datový proud zvuku a videa ze zařízení.

Aplikacím můžete ručně povolit příjem datového proudu zvuku a videa.

Speciální funkce ochrany datového proudu zvuku

Ochrana datového proudu zvuku má následující zvláštní znaky:

- Aby tato funkce pracovala, musí být povolena součást Prevence narušení hostitele.
- Pokud aplikace začala přijímat zvukový datový proud před spuštěním součásti Prevence narušení hostitele, aplikace Kaspersky Endpoint Security aplikaci povolí zvukový datový proud přijímat a nezobrazí žádné upozornění.
- Pokud aplikaci přesunete do skupiny Nedůvěryhodné nebo Vysoké omezení poté, co začala přijímat zvukový datový proud, software Kaspersky Endpoint Security aplikaci povolí zvukový datový proud přijímat a nezobrazí žádné upozornění.
- Po změně nastavení přístupu aplikace k zařízením pro záznam zvuku (například po zakázání příjmu zvukového datového proudu) je nutné aplikaci restartovat, aby došlo k zastavení příjmu zvukového datového proudu.
- Kontrola přístupu ke zvukovému datovému proudu ze zařízení pro záznam zvuku nezávisí na nastavení přístupu aplikace k webové kameře.
- Aplikace Kaspersky Endpoint Security chrání přístup pouze k integrovaným a externím mikrofonům. Jiná zařízení pro vysílání zvukových datových proudů nejsou podporována.
- Aplikace Kaspersky Endpoint Security nemůže zaručit ochranu zvukového datového proudu před zařízeními, jako jsou digitální fotoaparáty, kompaktní videokamery a sportovní kamery.
- Při prvním spuštění aplikací pro záznam či přehrávání zvuku nebo videa po nainstalování aplikace Kaspersky Endpoint Security může dojít k přerušení přehrávání nebo nahrávání zvuku či videa. Jedná se o nutný zásah aktivující funkci řídící přístup k zařízením pro záznam zvuku ze strany aplikací. Systémová služba, která řídí zvukový hardware, se při prvním spuštění aplikace Kaspersky Endpoint Security restartuje.

Speciální funkce ochrany přístupu k webové kameře aplikace

Ochrana přístupu k webové kameře má následující zvláštní požadavky a omezení:

- Aplikace kontroluje video a statické snímky vzniklé při zpracování dat z webové kamery.
- Pokud je součástí datového proudu videa webové kamery také datový proud zvuku, aplikace jej kontroluje.
- Aplikace kontroluje pouze webové kamery připojené prostřednictvím rozhraní USB nebo IEEE1394, které se ve správci zařízení systému Windows zobrazují jako **Zařízení pro zpracování obrázků**.
- Aplikace Kaspersky Endpoint Security podporuje následující webové kamery:
  - 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

Společnost Kaspersky nezaručuje podporu webových kamer, které nejsou v tomto seznamu uvedeny.

Modul pro nápravu

Součást Modul pro nápravu umožňuje aplikaci Kaspersky Endpoint Security vrátit zpět akce, které byly provedeny malwarem v operačním systému.

Při vracení změn provedených malwarem v operačním systému zpracuje aplikace Kaspersky Endpoint Security následující typy činností malwaru:

- **Činnost prováděná se soubory**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Odstraní spustitelné soubory, které byly vytvořeny malwarem (na všech médiích kromě síťových jednotek).
  - Odstraní spustitelné soubory, které byly vytvořeny programy, do nichž pronikl malware.
  - Obnoví soubory, které byly upraveny nebo odstraněny malwarem.

  Funkce obnovení souborů obsahuje řadu omezení.

- **Činnost prováděná v registru**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Odstraní klíče registru, které byly vytvořeny malwarem.
  - Neobnoví klíče registru, které byly upraveny nebo odstraněny malwarem.

- **Činnost systému**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Ukončí procesy, které byly zahájeny malwarem.
  - Ukončí procesy, do nichž pronikla nějaká škodlivá aplikace.

- Neobnoví procesy, které byly zastaveny malwarem.

- **Síťová aktivita**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Blokuje síťovou aktivitu malwaru.
  - Blokuje síťovou aktivitu procesů, do nichž pronikl malware.

Vrácení akcí malwaru může být zahájeno součástí Ochrana před souborovými hrozbami nebo Detekce chování nebo během antivirové kontroly.

Vrácení změn provedených malwarem má vliv na striktně definovanou sadu dat. Vrácení změn nemá žádný nežádoucí vliv na operační systém ani na integritu dat počítače.

Jak povolit nebo zakázat součást Modul pro nápravu v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Rozšířená ochrana před hrozbami → Modul pro nápravu**.
6. Pomocí zaškrtávacího políčka **Modul pro nápravu** můžete tuto součást povolit nebo zakázat.
7. Uložte změny.

Jak povolit nebo zakázat součást Modul pro nápravu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení → Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnost **Rozšířená ochrana před hrozbami → Modul pro nápravu**.
5. Pomocí přepínače **Modul pro nápravu** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

Jak povolit nebo zakázat součást Modul pro nápravu v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Modul pro nápravu**.
3. Pomocí přepínače **Modul pro nápravu** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je povolena součást Modul pro nápravu, aplikace Kaspersky Endpoint Security vrátí akce provedené škodlivými aplikacemi v operačním systému.

Služba hodnocení reputace KSN

Aby mohla aplikace Kaspersky Endpoint Security chránit váš počítač efektivněji, využívá data přijatá od uživatelů po celém světě. Pro přijímání těchto dat je určena služba Kaspersky Security Network.

Služba Kaspersky Security Network (KSN) představuje infrastrukturu cloudových služeb, která poskytuje přístup k internetové znalostní bázi společnosti Kaspersky s informacemi o reputaci souborů, webových prostředcích a softwaru. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikace Kaspersky Endpoint Security na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků. Jestliže se účastníte služby Kaspersky Security Network, služby KSN poskytují aplikaci Kaspersky Endpoint Security informace o kategorii a pověsti naskenovaných souborů a také informace o pověsti kontrolovaných webových adres.

Používání služby hodnocení reputace Kaspersky Security Network je dobrovolné. Aplikace vás vyzve k použití služby KSN během úvodní konfigurace aplikace. Uživatel může účast v programu KSN zahájit nebo ukončit kdykoli.

Podrobnější informace o statistických informacích generovaných při účasti v síti KSN, které jsou odesílány společnosti Kaspersky, a o uchovávání a likvidaci těchto informací najdete v prohlášení o službě Kaspersky Security Network a na webových stránkách společnosti Kaspersky. Soubor ksn_<ID jazyka>.txt s textem prohlášení o službě Kaspersky Security Network je součástí distribučního balíčku aplikace.

Za účelem snížení zatížení serverů služby KSN může společnost Kaspersky vydat aktualizace aplikace, které dočasně deaktivují nebo částečně omezí odesílání požadavků do služby Kaspersky Security Network. V tomto případě je stav připojení ke KSN v místním rozhraní aplikace *Povoleno s omezeními*.

Infrastruktura KSN

Aplikace Kaspersky Endpoint Security podporuje následující řešení infrastruktury KSN:

- *Globální KSN* je řešení, které používá většina aplikací Kaspersky. Účastníci služby Kaspersky Security Network získávají z této služby informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází pověsti a statistik služby Kaspersky Security Network.
- *Privátní KSN* je řešení, které umožňuje uživatelům počítačů, které jsou hostiteli aplikace Kaspersky Endpoint Security nebo jiných aplikací společnosti Kaspersky, získat přístup k databázím pověsti služby Kaspersky Security Network a k dalším statistickým údajům bez odesílání dat do KSN z vlastních počítačů. Možnost

privátní KSN je určena pro firemní zákazníky, kteří nemohou být součástí služby Kaspersky Security Network z některého z následujících důvodů:

- Místní pracovní stanice nejsou připojeny k internetu.
- Přenos jakýchkoli dat mimo zemi nebo mimo podnikovou síť LAN je zakázán zákonem nebo je omezen firemními bezpečnostními zásadami.

Ve výchozím nastavení aplikace Kaspersky Security Center používá globální KSN. Použití privátní služby KSN můžete nakonfigurovat v konzole pro správu (MMC) a webové konzole aplikace Kaspersky Security Center 12 a na příkazovém řádku. V cloudové konzole aplikace Kaspersky Security Center nelze součást používání privátní KSN konfigurovat.

Více informací o privátní KSN naleznete v *dokumentaci k aplikaci Kaspersky Private Security Network*.

Proxy server KSN

Uživatelské počítače spravované administračním serverem Kaspersky Security Center mohou se sítí KSN komunikovat prostřednictvím služby proxy serveru KSN.

Služba proxy serveru KSN poskytuje následující možnosti:

- Počítač uživatele může odesílat dotazy a informace do služby KSN i bez přímého přístupu k internetu.
- Služba proxy serveru KSN ukládá zpracovaná data do mezipaměti, čímž snižuje zatížení komunikačního kanálu a externí sítí a urychluje příjem informací, které jsou uživatelským počítačem požadovány.

Další informace o službě proxy serveru KSN najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

Povolení a zakázání používání služby Kaspersky Security Network

Postup povolení nebo zakázání používání služby Kaspersky Security Network:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Rozšířená ochrana před hrozbami → Kaspersky Security Network**.
3. Pomocí přepínače **Kaspersky Security Network** můžete součást povolit nebo zakázat.

   Pokud jste povolili použití KSN, aplikace Kaspersky Endpoint Security zobrazí prohlášení ke službě Kaspersky Security Network. Přečtěte si podmínky prohlášení ke službě Kaspersky Security Network (KSN), a pokud s nimi souhlasíte, přijměte jej.

   Ve výchozím nastavení Kaspersky Endpoint Security používá rozšířený režim KSN. *Rozšířený režim služby KSN* je režim, ve kterém aplikace Kaspersky Endpoint Security odesílá společnosti Kaspersky více údajů.
4. V případě potřeby přepínač **Povolit rozšířený režim KSN** vypněte.
5. Uložte změny.

Výsledkem je, že pokud je povoleno použití KSN, aplikace Kaspersky Endpoint Security používá informace o reputaci souborů, webových prostředků a aplikací přijatých ze služby Kaspersky Security Network.

Omezení privátní KSN

Privátní KSN (dále také KPSN) vám umožňuje používat ke kontrole reputace objektů (souborů nebo webových adres) vlastní lokální databázi reputace. Reputace objektu přidaného do místní databáze reputace má vyšší prioritu než reputace přidaná do KSN/KPSN. Představte si například, že aplikace Kaspersky Endpoint Security kontroluje počítač a vyžádá si reputaci souboru v KSN/KPSN. Pokud má soubor v místní databázi reputace reputaci „nedůvěryhodný“, ale v KSN/KPSN má reputaci „důvěryhodný“, aplikace Kaspersky Endpoint Security soubor detekuje jako „nedůvěryhodný“ a provede akci definovanou pro detekované hrozby.

V některých případech však aplikace Kaspersky Endpoint Security nemusí reputaci objektu v KSN/KPSN zjišťovat. V takovém případě nebude aplikace Kaspersky Endpoint Security přijímat data z místní databáze reputace KPSN. Aplikace Kaspersky Endpoint Security nemusí zjišťovat reputaci objektu v KSN/KPSN z následujících důvodů:

- Aplikace Kaspersky používají offline databáze reputace. Offline databáze reputace jsou navrženy tak, aby optimalizovaly prostředky během provozu aplikací Kaspersky a chránily kriticky důležité objekty v počítači. Offline databáze reputace jsou vytvářeny odborníky společnosti Kaspersky na základě dat ze sítě Kaspersky Security Network. Aplikace Kaspersky aktualizují offline databáze reputace antivirovými databázemi konkrétní aplikace. Pokud offline databáze reputace obsahují informace o kontrolovaném objektu, aplikace nepožaduje reputaci tohoto objektu od KSN/KPSN.

- Výjimky z kontroly (důvěryhodná zóna) se konfigurují v nastavení aplikace. V takovém případě aplikace nebere v úvahu reputaci objektu v místní databázi reputace.

- Aplikace používá technologie optimalizace kontroly, jako je iSwift nebo iChecker, nebo ukládá do mezipaměti požadavky na reputaci v
KSN/KPSN. V takovém případě nemusí aplikace zjišťovat reputaci dříve kontrolovaných objektů.

- Aby aplikace optimalizovala své pracovní vytížení, kontroluje soubory určitého formátu a velikosti. Seznam příslušných formátů a omezení velikosti určují odborníci společnosti Kaspersky. Tento seznam je aktualizován o antivirové databáze aplikace. Můžete také nakonfigurovat nastavení optimalizace kontroly v rozhraní aplikace, například pro součást Ochrana před souborovými hrozbami.

Povolení a zakázání režimu cloudu pro součásti ochrany

Cloudový režim znamená režim provozu aplikace, ve kterém Kaspersky Endpoint Security používá neúplnou verzi antivirových databází. Když se používají neúplné antivirové databáze, aplikace Kaspersky Security Network podporuje provoz aplikace. Neúplná verze antivirových databází vám umožňuje využívat přibližně polovinu paměti RAM počítače, která by se jinak využívala u obvyklých databází. Pokud se neúčastníte služby Kaspersky Security Network nebo pokud je cloudový režim vypnutý, Kaspersky Endpoint Security stáhne plnou verzi antivirových databází ze serverů společnosti Kaspersky.

Při použití služby Kaspersky Private Security Network je funkce režimu cloudu k dispozici od verze služby Kaspersky Private Security Network 3.0.

Povolení nebo zakázání režimu cloudu pro součásti ochrany:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Rozšířená ochrana před hrozbami** → **Kaspersky Security Network**.

3. Pomocí přepínače **Povolit režim cloudu** můžete tuto součást povolit nebo zakázat.

4. Uložte změny.

Aplikace Kaspersky Endpoint Security stáhne během příští aktualizace neúplnou verzi nebo plnou verzi antivirových databází.

Pokud není k dispozici použití neúplné verze antivirových databází, aplikace Kaspersky Endpoint Security automaticky přejde na prémiovou verzi antivirových databází.

Kontrola připojení ke službě Kaspersky Security Network

Připojení ke službě Kaspersky Security Network může být ztraceno z následujících důvodů:

- Nezapojili jste se do systému Kaspersky Security Network.
- Počítač není připojen k internetu.
- Aktuální stav klíče neumožňuje připojení ke službě Kaspersky Security Network. Připojení ke službě KSN nemusí být k dispozici například z následujících důvodů:
  - Aplikace není aktivována.
  - Platnost licence nebo předplatného vypršela.
  - Byly zjištěny problémy s licenčními klíči (například byl klíč přidán do seznamu zakázaných klíčů).

Postup kontroly připojení ke službě Kaspersky Security Network:

V hlavním okně aplikace klikněte na **Další nástroje** → **Kaspersky Security Network**.

Tím se otevře okno **Kaspersky Security Network**, v němž se zobrazují informace o aktivitě služby Kaspersky Security Network. Když je otevřeno okno **Kaspersky Security Network**, aplikace přijímá statistiky o využití služby KSN. Globální statistika cloudových služeb Kaspersky Security Network a čas synchronizace nejsou aktualizovány v reálném čase.

V levé části okna **Kaspersky Security Network** se zobrazuje jeden z následujících stavů pro připojení mezi počítačem a službou Kaspersky Security Network:

- *Povoleno.*

  Tento stav znamená, že během operací aplikace Kaspersky Endpoint Security je používána služba Kaspersky Security Network a servery služby KSN jsou k dispozici.

- *Povoleno. Dostupné s omezeními.*

  Tento stav znamená, že během operací aplikace Kaspersky Endpoint Security je používána služba Kaspersky Security Network a servery služby KSN nejsou k dispozici.

  Servery KSN nemusí být k dispozici z následujících důvodů:

  - V počítači je spuštěna služba KSN Proxy (ksnproxy).

- Brána firewall blokuje port 13111.

Pokud doba, která uplynula od poslední synchronizace se servery služby KSN překročí 15 minut nebo je u ní zobrazen *neznámý* stav, stav připojení aplikace Kaspersky Endpoint Security ke službě Kaspersky Security Network má hodnotu *Povoleno. Nedostupný*.

- *Vyp.*

  Tento stav znamená, že během operací aplikace Kaspersky Endpoint Security není používána služba Kaspersky Security Network.

Pokud připojení k serverům služby Kaspersky Security Network nelze obnovit, doporučuje se kontaktovat technickou podporu nebo poskytovatele služeb.

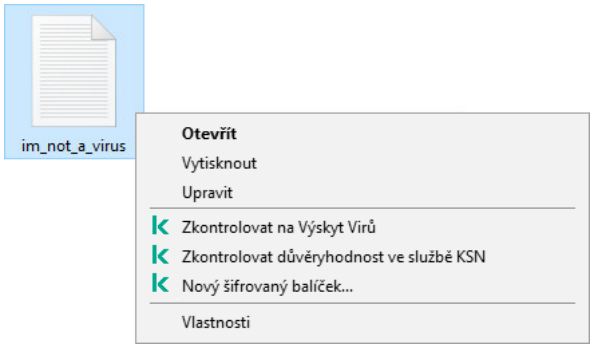
Kontrola důvěryhodnosti souboru ve službě Kaspersky Security Network

Pokud pochybujete o bezpečnosti souboru, můžete zkontrolovat jeho důvěryhodnost ve službě Kaspersky Security Network.

Pokud jste přijali podmínky prohlášení týkající se služby Kaspersky Security Network, můžete zkontrolovat reputaci souboru.

Postup kontroly důvěryhodnosti souboru ve službě Kaspersky Security Network:

Otevřete místní nabídku souboru a vyberte možnost **Kontrola reputace v KSN** (viz obrázek níže).



Místní nabídka Soubor

Aplikace Kaspersky Endpoint Security zobrazuje důvěryhodnost souboru:

Důvěryhodné. Většina uživatelů služby Kaspersky Security Network potvrdila důvěryhodnost souboru.

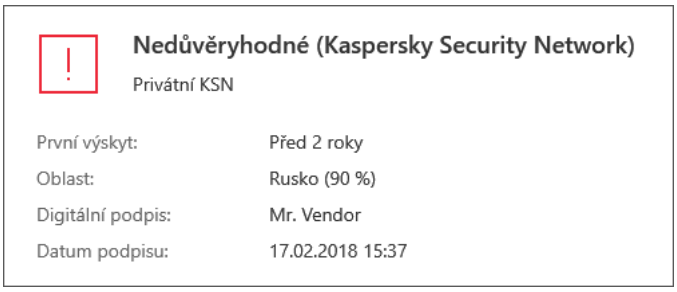
Legitimní software, který lze využít k poškození počítače nebo osobních údajů. I když tyto aplikace nemají žádnou škodlivou funkci, mohou být zneužity útočníky. Podrobnosti o legitimním softwaru, který může být využíván pachateli k poškození počítače nebo osobních údajů uživatele, najdete na webových stránkách encyklopedie IT Kaspersky. Tyto aplikace můžete přidat na seznam důvěryhodných zařízení.

Nedůvěryhodné. Virus nebo jiná aplikace, které představují hrozbu.

Není známo. Kaspersky Security Network nemá o souboru žádné informace. Soubor můžete zkontrolovat pomocí antivirových databází (v místní nabídce možnost **Zkontrolovat na výskyt virů**).

Aplikace Kaspersky Endpoint Security zobrazuje řešení KSN, které bylo použito k určení důvěryhodnosti souboru: *Globální KSN* nebo *Privátní KSN*.

Aplikace Kaspersky Endpoint Security také zobrazuje další informace o souboru (viz obrázek níže).



Důvěryhodnost souboru ve službě Kaspersky Security Network

Kontrola šifrovaného připojení

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Po instalaci přidá aplikace Kaspersky Endpoint Security certifikát Kaspersky do systémového úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Aplikace Kaspersky Endpoint Security také zahrnuje použití systémového úložiště důvěryhodných certifikátů v prohlížečích Firefox a Thunderbird ke kontrole provozu těchto aplikací.

Součásti Kontrola webu, Ochrana před hrozbami v poště a Ochrana před webovými hrozbami mohou dešifrovat a kontrolovat síťový provoz přenášený pomocí šifrovaných připojení prostřednictvím následujících protokolů:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Konfigurace nastavení kontroly šifrovaných připojení

Postup konfigurace nastavení kontroly šifrovaných připojení:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.
3. V části Kontrola šifrovaných připojení vyberte režim kontroly šifrovaných připojení:
   - **Nekontrolovat šifrovaná připojení** Aplikace Kaspersky Endpoint Security nebude mít přístup k obsahu webů, jejichž adresa začíná na `https://`.

- **Kontrolovat šifrovaná připojení na žádost odeslanou součástmi ochrany**. Aplikace Kaspersky Endpoint Security bude kontrolovat šifrované přenosy, pouze pokud o to požádají součásti Ochrana před souborovými hrozbami, Ochrana před hrozbami v poště nebo Kontrola webu.

- **Vždy kontrolovat šifrovaná připojení** Aplikace Kaspersky Endpoint Security bude kontrolovat šifrovaný provoz, i když jsou zakázány součásti ochrany.

Aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení vytvořená důvěryhodnými aplikacemi, pro které je kontrola provozu zakázána. Aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení z předdefinovaného seznamu důvěryhodných webů. Předdefinovaný seznam důvěryhodných webů vytvářejí odborníci společnosti Kaspersky. Tento seznam je aktualizován o antivirové databáze aplikace. Předdefinovaný seznam důvěryhodných webů můžete zobrazit pouze v rozhraní aplikace Kaspersky Endpoint Security. Seznam nemůžete zobrazit v konzole aplikace Kaspersky Security Center.

4. V případě potřeby přidejte výjimky z kontroly: důvěryhodné adresy a aplikace.

5. Klikněte na tlačítko **Rozšířené nastavení**.

6. Nakonfigurujte nastavení pro kontrolu šifrovaných připojení (viz tabulka níže).

7. Uložte změny.

Nastavení kontroly šifrovaných připojení

Parametr	Popis
Při návštěvě domény s nedůvěryhodným certifikátem	• **Povolit**. Pokud je vybrána tato možnost, při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security povolí síťové připojení. Při otevření domény s nedůvěryhodným certifikátem v prohlížeči zobrazí aplikace Kaspersky Endpoint Security stránku HTML s upozorněním a důvodem toho, proč není návštěva dané domény doporučena. Uživatel může kliknout na odkaz na stránce HTML s upozorněním, aby získal přístup k požadovanému webovému prostředku. Po přejití na odkaz nebude aplikace Kaspersky Endpoint Security během další hodiny v případě návštěvy jiných prostředků v této stejné doméně zobrazovat upozornění na nedůvěryhodný certifikát. • **Blokovat připojení**. Pokud je vybrána tato možnost, při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security blokuje síťové připojení. Při otevření domény s nedůvěryhodným certifikátem v prohlížeči zobrazí aplikace Kaspersky Endpoint Security stránku HTML s důvodem toho, proč je daná doména blokována.
Při výskytu chyb kontroly šifrovaného připojení	• **Blokovat připojení**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení blokuje síťové připojení. • **Přidat doménu do výjimek**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení přidá doménu, v jejímž důsledku došlo k chybě, do seznamu výjimek s chybami kontroly a při návštěvě této domény nesleduje šifrovaný síťový provoz. Seznam domén s chybami kontroly šifrovaného připojení můžete

	zobrazit pouze v místním rozhraní aplikace. Chcete-li vymazat obsah seznamu, musíte vybrat možnost **Blokovat připojení**.
Blokovat připojení SSL 2.0	Pokud je políčko zaškrtnuto, aplikace Kaspersky Endpoint Security blokuje síťová připojení vytvořená pomocí protokolu SSL 2.0. Pokud políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security neblokuje síťová připojení vytvořená pomocí protokolu SSL 2.0 a nesleduje síťový provoz přenášený pomocí těchto připojení.
Dešifrovat šifrovaná připojení u webů používajících certifikáty EV	Certifikáty EV (Extended Validation Certificate) potvrzují pravost webových stránek a zvyšují bezpečnost připojení. K označení, že web má certifikát EV, používají prohlížeče ikonu zámku v adresním řádku. Prohlížeče mohou pruh adresy také plně nebo částečně vybarvit zelenou barvou. Pokud je toto políčko zaškrtnuté, aplikace Kaspersky Endpoint Security dešifruje a monitoruje šifrovaná připojení a weby, které používají certifikát EV. Jestliže toto políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security nemá přístup k obsahu provozu HTTPS. Z tohoto důvodu aplikace monitoruje provoz HTTPS pouze na základě adresy webových stránek, například, `https://facebook.com`. Pokud poprvé otevíráte web s certifikátem EV, šifrované připojení bude dešifrováno bez ohledu na to, zda je toto políčko zaškrtnuto.

Kontrola šifrovaného připojení ve Firefoxu a Thunderbirdu

Po instalaci přidá aplikace Kaspersky Endpoint Security certifikát Kaspersky do systémového úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Ve výchozím nastavení používají Firefox a Thunderbird místo úložiště certifikátů Windows vlastní proprietární úložiště certifikátů Mozilla. Pokud je ve vaší organizaci nasazena aplikace Kaspersky Security Center a na počítač se používají zásady, aplikace Kaspersky Endpoint Security automaticky povolí použití úložiště certifikátů Windows ve Firefoxu a Thunderbirdu ke kontrole provozu těchto aplikací. Pokud se žádná zásada na počítač nepoužívá, můžete si vybrat úložiště certifikátů, které budou aplikace Mozilla používat. Pokud jste vybrali úložiště certifikátů Mozilla, ručně do něj přidejte certifikát Kaspersky. To zabrání chybám při práci s přenosy HTTPS.

Chcete-li kontrolovat provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird, musíte povolit kontrolu šifrovaného připojení. Je-li kontrola šifrovaného připojení zakázána, aplikace Kaspersky Endpoint Security nekontroluje šifrovaný provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird.

Před přidáním certifikátu do úložiště Mozilly exportujte certifikát Kaspersky z ovládacího panelu systému Windows (vlastnosti prohlížeče). Podrobnosti o exportu certifikátu Kaspersky najdete ve znalostní bázi technické podpory. Podrobnosti o přidání certifikátu do úložiště najdete na *webu technické podpory Mozilly*.

Úložiště certifikátů si můžete vybrat pouze v místním rozhraní aplikace.

Výběr úložiště certifikátů pro kontrolu šifrovaných připojení ve Firefoxu a Thunderbirdu:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V bloku **Mozilla Firefox a Thunderbird** zaškrtněte políčko **Kontrolovat zabezpečené přenosy v aplikacích Mozilla**.

4. Vyberte úložiště certifikátů:

   - **Použít úložiště certifikátů Windows**. Kořenový certifikát společnosti Kaspersky bude přidán do tohoto úložiště během instalace aplikace Kaspersky Endpoint Security.

   - **Použít úložiště certifikátů prohlížeče Mozilla**. Mozilla Firefox a Thunderbird používají svá vlastní úložiště certifikátů. Pokud je vybráno úložiště certifikátů Mozilla, musíte do tohoto úložiště ručně přidat kořenový certifikát společnosti Kaspersky prostřednictvím vlastností prohlížeče.

5. Uložte změny.

Vyloučení šifrovaných připojení z kontroly

Většina webových zdrojů používá šifrovaná připojení. Odborníci společnosti Kaspersky doporučují povolit kontrolu šifrovaných připojení. Pokud kontrola šifrovaných připojení narušuje pracovní činnost, můžete přidat web k výjimkám označovaným jako *důvěryhodné adresy*. Jestliže důvěryhodná aplikace používá šifrované připojení, můžete u této aplikaci zakázat kontrolu šifrovaných připojení. Můžete například zakázat kontrolu šifrovaných připojení u aplikací cloudového úložiště, které používají dvoustupňové ověřování s vlastním certifikátem.

Postup vyloučení webové adresy z kontroly šifrovaných připojení:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V části **Kontrola šifrovaného připojení** klikněte na tlačítko **Důvěryhodné adresy**.

4. Klikněte na tlačítko **Přidat**.

5. Zadejte název domény nebo IP adresu, pokud nechcete, aby aplikace Kaspersky Endpoint Security kontrolovala šifrovaná připojení vytvořená při návštěvě dané domény.

   Kaspersky Endpoint Security podporuje při zadávání masky názvu domény znak `*`.

   > Aplikace Kaspersky Endpoint Security nepodporuje masky pro IP adresy.

   Příklady:

   - `domena.cz` – tato položka zahrnuje následující adresy: `https://domena.cz`, `https://www.domena.cz`, `https://domena.cz/stranka123`. Tato položka nezahrnuje subdomény (například, `subdomena.domena.cz`).

   - `subdomena.domena.cz` – tato položka zahrnuje následující adresy: `https://subdomena.domena.cz`, `https://subdomena.domena.cz/stranka123`. Tato položka nezahrnuje doménu `domena.cz`.

   - `*.domena.cz` – tato položka zahrnuje následující adresy: `https://filmy.domena.cz`, `https://obrazky.domena.cz/stranka123`. Tato položka nezahrnuje doménu `domena.cz`.

6. Uložte změny.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení v případě výskytu chyb a přidá web na zvláštní seznam *domén s chybami kontroly*. Aplikace Kaspersky Endpoint Security sestavuje samostatný seznam pro každého uživatele a neodesílá data do aplikace Kaspersky Security Center. V případě chyby kontroly můžete povolit blokování připojení. Seznam domén s chybami kontroly šifrovaného připojení můžete zobrazit pouze v místním rozhraní aplikace.

- Uložte změny.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení v případě výskytu chyb a přidá web na zvláštní seznam *domén s chybami kontroly*. Aplikace Kaspersky Endpoint Security sestavuje samostatný seznam pro každého uživatele a neodesílá data do aplikace Kaspersky Security Center. V případě chyby kontroly můžete povolit blokování připojení. Seznam domén s chybami kontroly šifrovaného připojení můžete zobrazit pouze v místním rozhraní aplikace.

Zobrazení seznamu domén s chybami kontroly:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V části **Kontrola šifrovaného připojení** klikněte na tlačítko **Domény s chybami kontroly**.

   Otevře se seznam domén s chybami kontroly. Chcete-li seznam obnovit, povolte v zásadě blokování připojení při chybě kontroly, použijte zásadu, pak resetujte parametr na jeho počáteční hodnotu a znovu použijte zásadu.

Odborníci společnosti Kaspersky vytvářejí seznam *globálních výjimek*, což jsou důvěryhodné weby, které Kaspersky Endpoint Security nekontroluje bez ohledu na nastavení aplikace.

Postup zobrazení globálních výjimek z kontroly šifrovaného síťového provozu:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V části **Kontrola šifrovaného připojení** klikněte na odkaz **weby**.

   Otevře se seznam webů sestavený odborníky společnosti Kaspersky. Aplikace Kaspersky Endpoint Security nekontroluje u webů na seznamu chráněná připojení. Seznam lze aktualizovat během aktualizace databází a modulů aplikace Kaspersky Endpoint Security.

Kontrola webu

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Kontrola webu řídí přístup uživatelů k webovým prostředkům. To pomáhá omezit provoz a nevhodné využití pracovní doby. Když se uživatel pokusí otevřít web, k němuž omezuje přístup součást Kontrola webu, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).

Aplikace Kaspersky Endpoint Security sleduje pouze provoz HTTP a HTTPS.

Pro sledování provozu HTTPS je třeba povolit kontroly šifrovaných připojení.

Metody pro správu přístupu k webům

Kontrola webu umožňuje konfigurovat přístup k webům následujícími způsoby:

- **Kategorie webu**. Weby jsou tříděny podle cloudové služby Kaspersky Security Network, heuristické analýzy a databáze známých webů (jedna z databází aplikace). Můžete například omezit přístup uživatelů ke kategorii „Sociální sítě“ nebo jiným kategoriím.
- **Typ dat**. Můžete omezit přístup uživatelů k datům na webu a skrýt například grafické obrázky. Aplikace Kaspersky Endpoint Security určuje typ dat na základě formátu souboru, a ne na základě jeho přípony.

  Aplikace Kaspersky Endpoint Security nekontroluje soubory v archivech. Pokud byly například obrazové soubory umístěny do archivu, aplikace Kaspersky Endpoint Security identifikuje datový typ „Archivy“, nikoli „Grafické soubory“.

- **Jednotlivé adresy**. Můžete zadat webovou adresu nebo použít masky.

Pro regulaci přístupu na webové stránky můžete současně použít několik způsobů. Můžete například omezit přístup ke kategorii webu „Soubory sady Office“ pouze pro kategorii webových stránek „Webový e-mail“.

Pravidla přístupu k webu

Součást Kontrola zařízení řídí přístup uživatelů k zařízením pomocí *pravidel přístupu*. Pro pravidlo přístupu k webu můžete nakonfigurovat následující rozšířená nastavení:

- Uživatelé, na které se pravidlo vztahuje.

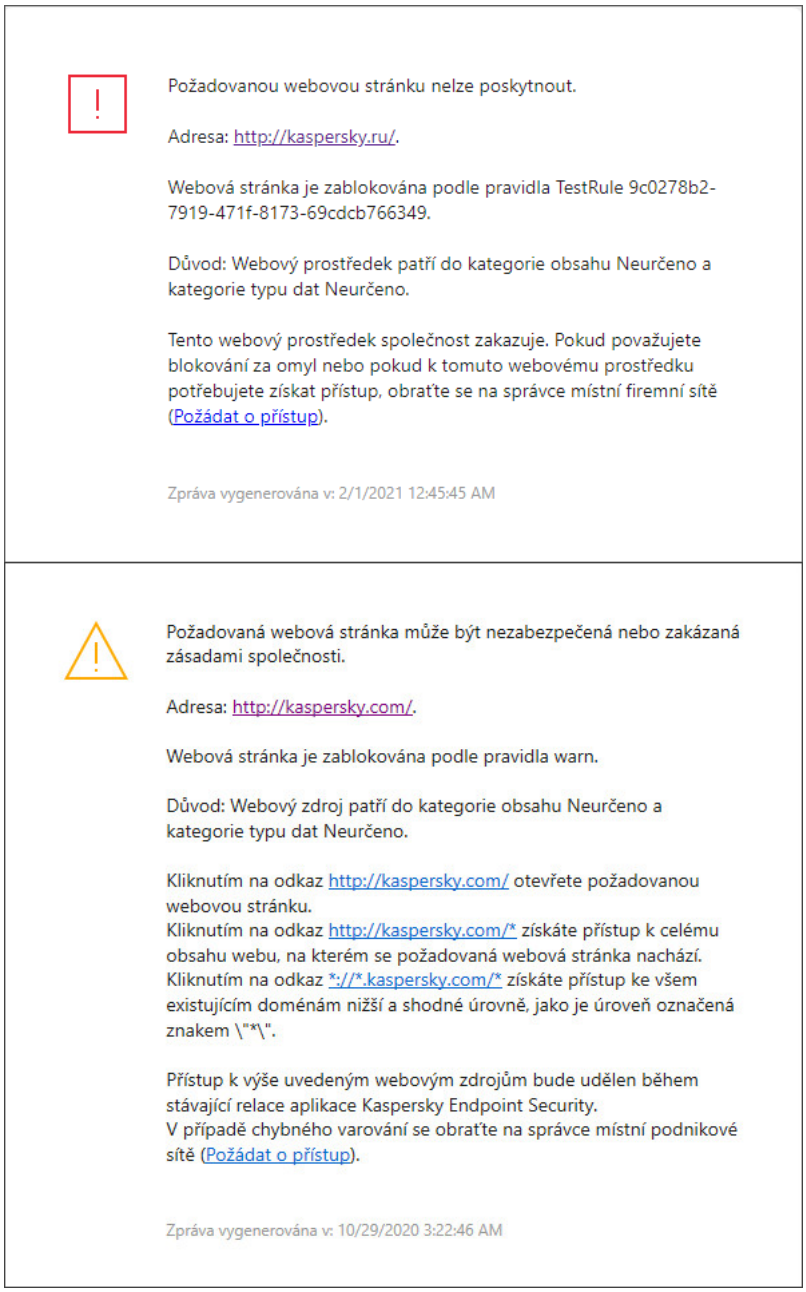
  Můžete například omezit přístup k internetu prostřednictvím prohlížeče pro všechny uživatele společnosti kromě IT oddělení.

- Plán pravidel.

Můžete například omezit přístup k internetu prostřednictvím prohlížeče pouze v pracovní době.

Priority pravidel přístupu

Každé pravidlo má prioritu. Čím výše se pravidlo na seznamu nachází, tím vyšší je jeho priorita. Pokud byl web přidán do více pravidel, řídí součást Kontrola webu přístup k webu na základě pravidla s nejvyšší prioritou. Aplikace Kaspersky Endpoint Security může například identifikovat firemní portál jako sociální síť. Chcete-li omezit přístup k sociálním sítím a poskytnout přístup k firemnímu webovému portálu, vytvořte dvě pravidla: jedno pravidlo blokující kategorii webových stránek „Sociální sítě“ a jedno pravidlo povolující firemní webový portál. Pravidlo přístupu pro firemní webový portál musí mít vyšší prioritu než pravidlo přístupu pro sociální sítě.



Zprávy součástí Kontrola webu

Povolení a zakázání součásti Kontrola webu

Součást Kontrola webu je ve výchozím nastavení povolena.

Postup povolení nebo zakázání součásti Kontrola webu:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.
3. Pomocí přepínače **Kontrola webu** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Akce prováděné s pravidly přístupu k webovým prostředkům

Nedoporučujeme vytvářet více než 1 000 pravidel přístupu k webovým prostředků, protože to může způsobit nestabilitu systému.

Pravidlo přístupu k webovým prostředkům je sada filtrů a akcí, které aplikace Kaspersky Endpoint Security provádí, když uživatel navštíví webové prostředky popsané v pravidle během doby uvedené v plánu pravidla. Filtry umožňují přesně zadat fond webových prostředků, u nichž je přístup kontrolovaný součástí Kontrola webu.

K dispozici jsou následující filtry:

- **Filtrování podle obsahu**. Součást Kontrola webu řadí do kategorií webové prostředky podle obsahu a typu dat. Můžete určovat přístup uživatelů k webovým prostředkům s obsahem a daty spadajícími do typů definovaných těmito kategoriemi. Když uživatelé navštíví webové prostředky patřící do vybrané kategorie obsahu a/nebo typu dat, aplikace Kaspersky Endpoint Security provede akci, která je zadaná v pravidle.
- **Filtrování podle adres webových prostředků**. Můžete určovat přístup uživatelů ke všem adresám webových prostředků nebo jednotlivým adresám webových prostředků a/nebo skupinám adres webových prostředků.

  Pokud je zadáno filtrování podle obsahu a filtrování podle adres webových prostředků a zadané adresy webových prostředků a/nebo skupiny adres webových prostředků patří do vybraných kategorií obsahu nebo typu dat, aplikace Kaspersky Endpoint Security neurčuje přístup ke všem webovým prostředkům ve vybraných kategoriích obsahu a/nebo kategoriích typu dat. Místo toho tato aplikace kontroluje přístup jen k zadaným adresám webových prostředků a/nebo skupinám adres webových prostředků.
- **Filtrování podle jmen uživatelů a skupin uživatelů**. Můžete zadat jména uživatelů a/nebo skupin uživatelů, u nichž je přístup k webovým prostředkům řízen pravidlem.
- **Plán pravidel** Můžete zadat plán pravidla. Plán pravidla určuje časové rozmezí, během kterého sleduje aplikace Kaspersky Endpoint Security přístup k webovým prostředkům, na které se pravidlo vztahuje.

Po instalaci aplikace Kaspersky Endpoint Security není seznam pravidel součásti Kontrola webu prázdný. Jsou předem nastavena dvě pravidla:

- Pravidlo Skripty a šablony stylů, které uděluje přístup v kteroukoli dobu všem uživatelům k webovým prostředkům, jejichž adresa obsahuje názvy souborů s příponami CSS, JS nebo VBS. Například: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.
- Výchozí pravidlo. Toto pravidlo se použije na jakékoli webové prostředky, kterých se netýkají jiná pravidla, a pro všechny uživatele povolí nebo blokuje přístup k těmto webovým prostředkům.

Přidání pravidla přístupu k webovým prostředkům

Postup přidání nebo úpravy pravidla přístupu k webovým prostředkům:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.
3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
4. V daném okně klikněte na tlačítko **Přidat**.

   Otevře se okno **Pravidlo přístupu k webovým prostředkům**.
5. V poli **Název pravidla** zadejte název pravidla.
6. U pravidla přístupu k webovému prostředku vyberte stav **Aktivní**.

   Pomocí přepínače můžete kdykoli zakázat pravidlo přístupu k webovým prostředkům.
7. V bloku **Akce** vyberte příslušnou možnost:

   - **Povolit**. Pokud je vybrána tato hodnota, povolí aplikace Kaspersky Endpoint Security přístup k webovým prostředkům, které odpovídají parametrům pravidla.
   - **Blokovat**. Pokud je vybrána tato hodnota, zablokuje aplikace Kaspersky Endpoint Security přístup k webovým prostředkům, které odpovídají parametrům pravidla.
   - **Varovat**. Pokud vyberete tuto hodnotu, aplikace Kaspersky Endpoint Security zobrazí upozornění na to, že je některý webový prostředek nežádoucí, jestliže se uživatel pokusí o přístup k webovým prostředkům odpovídajícím pravidlu. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.
8. V bloku **Typ filtru** vyberte příslušný filtr obsahu:

   - **Podle kategorií obsahu**. Přístup uživatelů k webovým prostředkům můžete ovládat podle kategorie (například kategorie *Sociální sítě*).
   - **Podle typů dat**. Můžete řídit přístup uživatele k webovým prostředkům na základě konkrétního datového typu jeho publikovaných dat (například *Grafické obrázky*).

   Postup konfigurace filtru obsahu:

   a. Klikněte na odkaz **Konfigurovat**.

   b. Zaškrtněte políčka u názvů požadovaných kategorií obsahu a/nebo typů dat.

   Zaškrtnutí políčka vedle názvu kategorie obsahu a/nebo typu dat znamená, že aplikace Kaspersky Endpoint Security použije dané pravidlo při řízení přístupu k webovým prostředkům, které patří do vybraných kategorií obsahu a/nebo typů dat.

   c. Vraťte se do okna pro konfiguraci pravidla přístupu k webovým prostředkům.
9. V bloku **Adresy** vyberte příslušný filtr adres webového prostředku:

   - **Na všechny adresy**. Kontrola webu nebude filtrovat webové zdroje podle adresy.

- **Na jednotlivé adresy**. Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Vytvoření seznamu adres webových prostředků:

  a. Klikněte na tlačítko **Přidat adresu** nebo **Přidat skupinu adres**.

  b. V okně, které se otevře, vytvořte seznam adres webových prostředků. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT.

  c. Vraťte se do okna pro konfiguraci pravidla přístupu k webovým prostředkům.

  Pokud je zakázána kontrola šifrovaných připojení, v případě protokolu HTTPS můžete filtrovat pouze podle názvu serveru.

10. V bloku **Uživatelé** vyberte příslušný filtr pro uživatele:

    - **Na všechny uživatele**. Kontrola webu nebude filtrovat webové zdroje pro konkrétní uživatele.
    - **Na jednotlivé uživatele a/nebo skupiny**. Kontrola webu bude filtrovat webové zdroje pouze pro konkrétní uživatele. Vytvoření seznamu uživatelů, na které chcete pravidlo použít:

      a. Klikněte na tlačítko **Přidat**.

      b. V okně, které se otevře, vyberte uživatele nebo skupinu uživatelů, na které chcete použít pravidlo přístupu k webovému prostředku.

      c. Vraťte se do okna pro konfiguraci pravidla přístupu k webovým prostředkům.

11. V rozevíracím seznamu **Plán pravidel** vyberte název požadovaného plánu nebo vygenerujte nový plán na základě vybraného plánu pravidla. Postup:

    a. Klikněte na tlačítko **Správa plánu**.

    b. V daném okně klikněte na tlačítko **Přidat**.

    c. V okně, které se otevře, zadejte název plánu pravidel.

    d. Nakonfigurujte plán přístupu k webovým prostředkům pro uživatele.

    e. Vraťte se do okna pro konfiguraci pravidla přístupu k webovým prostředkům.

12. Uložte změny.

Přiřazení priorit k pravidlům přístupu k webovým prostředkům

Uspořádáním pořadí pravidel můžete přiřadit prioritu ke každému pravidlu na seznamu pravidel.

Přiřazení priority k pravidlu přístupu k webovým prostředkům:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.

3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
4. V okně, které se otevře, vyberte pravidlo, jehož prioritu chcete změnit.
5. Pomocí tlačítek **Nahoru** a **Dolů** přesuňte pravidlo na příslušné místo v seznamu pravidel přístupu k webovým prostředkům.
6. Uložte změny.

Povolení a zakázání pravidla přístupu k webovým prostředkům

Postup povolení a zakázání pravidla přístupu k webovým prostředkům:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.
3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
4. V okně, které se otevře, vyberte pravidlo, které chcete povolit nebo zakázat.
5. Ve sloupci **Stav** proveďte následující akci:
   - Pokud chcete použití pravidla povolit, vyberte hodnotu **Aktivní**.
   - Pokud chcete použití pravidla zakázat, vyberte hodnotu **Neaktivní**.
6. Uložte změny.

Export a import seznamu důvěryhodných webových adres

Seznam pravidel součásti Správa webových zásad můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství adres stejného typu. Můžete použít funkci exportu/importu k zálohování seznamu pravidel součásti Správa webových zásad nebo k migraci seznamu na jiný server.

Jak exportovat a importovat seznam pravidel součásti Správa webových zásad v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Kontrolní prvky zabezpečení** → **Správa webových zásad**.
6. Postup exportu seznamu pravidel součásti Správa webových zásad:
   a. Vyberte pravidla, která chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádné pravidlo nevybrali, aplikace Kaspersky Endpoint Security exportuje všechna pravidla.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
7. Postup importu seznamu pravidel součásti Správa webových zásad:
   a. Klikněte na odkaz **Importovat**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

[Jak exportovat a importovat seznam pravidel součásti Správa webových zásad ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam pravidel.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Kontrolní prvky zabezpečení** → **Správa webových zásad**.
5. Postup exportu seznamu pravidel v bloku **Seznam pravidel**:

   a. Vyberte pravidla, která chcete exportovat.

   b. Klikněte na tlačítko **Exportovat**.

   c. Potvrďte, jestli chcete exportovat pouze vybraná pravidla, nebo exportovat celý seznam pravidel.

   d. Klikněte na tlačítko **Exportovat**.

   Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML ve výchozí složce pro stahování.
6. Postup importu seznamu pravidel v bloku **Seznam pravidel**:

   a. Klikněte na odkaz **Importovat**.

   V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.

   b. Klikněte na tlačítko **Otevřít**.

   Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
7. Uložte změny.

Testování pravidel přístupu k webovým prostředkům

Chcete-li zkontrolovat konzistenci pravidel součásti Kontrola webu, můžete je otestovat. Součást Kontrola webu nabízí k tomuto účelu funkci Diagnostika pravidel.

Postup testování pravidel přístupu k webovým prostředkům:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.
3. V bloku **Nastavení** klikněte na odkaz **Diagnostika pravidel**.

   Otevře se okno **Diagnostika pravidel**.
4. Pokud chcete otestovat pravidla, která používá aplikace Kaspersky Endpoint Security k řízení přístupu k určitému webovému prostředku, zaškrtněte políčko **Zadejte adresu**. Do pole níže zadejte adresu webového prostředku.

5. Pokud chcete otestovat pravidla, která používá aplikace Kaspersky Endpoint Security k řízení přístupu k webovým prostředkům pro určité uživatele a/nebo skupiny uživatelů, zadejte seznam uživatelů a/nebo skupin uživatelů.

6. Pokud chcete otestovat pravidla, která používá aplikace Kaspersky Endpoint Security k řízení přístupu k webovým prostředkům se zadanými kategoriemi obsahu a/nebo kategoriemi typů dat, vyberte v rozevíracím seznamu **Filtrovat obsah** požadovanou možnost (**Podle kategorií obsahu**, **Podle typů dat** nebo **Podle kategorií obsahu a typů dat**).

7. Pokud chcete otestovat pravidla s informacemi o čase a dni v týdnu, kdy se uskutečnil pokus o přístup k webovým prostředkům zadaným v podmínkách diagnostiky pravidla, zaškrtněte políčko **Vložit čas pokusu o přístup**. Potom zadejte den v týdnu a čas.

8. Klikněte na tlačítko **Test**.

Po dokončení testu se zobrazí zpráva s informacemi o akci provedené aplikací Kaspersky Endpoint Security v souladu s prvním pravidlem aktivovaným při pokusu o přístup k zadanému webovému prostředku (Povolit, Blokovat nebo Varovat). První pravidlo, které se aktivuje, je to, které je na seznamu pravidel součásti Kontrola webu na vyšší pozici než ostatní pravidla splňující podmínky diagnostiky. Zpráva se zobrazí vpravo od tlačítka **Test**. V následující tabulce jsou uvedena zbývající aktivovaná pravidla společně s akcí prováděnou aplikací Kaspersky Endpoint Security. Pravidla jsou uvedena v pořadí podle sestupné priority.

Export a import seznamu adres webových prostředků

Pokud jste vytvořili seznam adres webových prostředků v pravidle přístupu k webovým prostředkům, můžete jej exportovat do souboru .txt. Seznam v tomto souboru můžete potom importovat, abyste nemuseli při konfiguraci pravidla přístupu vytvářet nový seznam adres webových prostředků ručně. Možnost pro export a import seznamu adres webových prostředků může být užitečná, když například vytváříte pravidla s podobnými parametry.

Postup importu nebo exportu seznamu adres webových prostředků do souboru:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.

3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.

4. Vyberte pravidlo, jehož seznam adres webových prostředků chcete exportovat nebo importovat.

5. Chcete-li exportovat seznam důvěryhodných webových adres, proveďte v bloku **Adresy** následující akce:

   a. Vyberte adresy, které chcete exportovat.

   Pokud jste nevybrali žádnou adresu, aplikace Kaspersky Endpoint Security exportuje všechny adresy.

   b. Klikněte na tlačítko **Exportovat**.

   c. V okně, které se otevře, zadejte název souboru TXT, do kterého chcete exportovat seznam důvěryhodných adres webových prostředků, a vyberte složku, do které chcete tento soubor uložit.

   d. Klikněte na tlačítko **Uložit**.

   Aplikace Kaspersky Endpoint Security exportuje seznam adres webových prostředků do souboru TXT.

6. Chcete-li importovat seznam webových prostředků, proveďte v bloku **Adresy** následující akce:

   a. Klikněte na tlačítko **Importovat**.

V okně, které se otevře, vyberte soubor TXT, ze kterého chcete importovat seznam webových prostředků.

b. Klikněte na tlačítko **Otevřít**.

Pokud počítač již seznam adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.

7. Uložte změny.

Sledování aktivity uživatelů na internetu

Aplikace Kaspersky Endpoint Security umožňuje protokolovat data o návštěvách uživatelů na všech webech, včetně povolených webů. To vám umožní získat úplnou historii zobrazení v prohlížeči. Kaspersky Endpoint Security odesílá události aktivity uživatele do aplikace Kaspersky Security Center, do místního protokolu aplikace Kaspersky Endpoint Security a do protokolu událostí systému Windows. Chcete-li přijímat události v aplikaci Kaspersky Security Center, je třeba nakonfigurovat nastavení událostí v zásadách v konzole pro správu nebo webové konzole. Můžete také nakonfigurovat přenos událostí součásti Kontrola webu e-mailem a zobrazování upozornění na obrazovce v počítači uživatele.

Aplikace Kaspersky Endpoint Security vytváří následující události aktivity uživatele na internetu:

- Blokování webů (stav *Kritické události*).
- Návštěva nedoporučeného webu (Stav *Varování*).
- Návštěva povolených webových stránek (stav *Informační zprávy*).

Před povolením sledování aktivity uživatele na internetu musíte provést následující:

- Vložit skript interakce s webovou stránkou do webového provozu (viz pokyny níže). Skript umožňuje registraci událostí součásti Kontrola webu.
- Pro sledování provozu HTTPS je třeba povolit kontroly šifrovaných připojení.

Postup vložení skriptu interakce s webovou stránkou do webového provozu:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.
3. V bloku **Zpracování provozu** zaškrtněte políčko **Vložit interakční skript do provozu**.
4. Uložte změny.

Aplikace Kaspersky Endpoint Security tak do webového provozu vloží skript interakce s webovou stránkou. Tento skript umožňuje evidenci událostí součásti Kontrola webu pro protokol událostí aplikace, protokol událostí OS a zprávy.

Postup konfigurace protokolování událostí součásti Kontrola webu v počítači uživatele:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně s nastavením aplikace vyberte část **Rozhraní**.

3. V části **Upozornění** klikněte na tlačítko **Pravidla pro upozornění**.

4. V okně, které se otevře, vyberte část **Kontrola webu**.

   Tím se otevře tabulka událostí součásti Kontrola webu a způsobů oznamování.

5. Nakonfigurujte metodu oznamování pro každou událost: **Uložit do místní zprávy** nebo **Uložit do protokolu událostí systému Windows**.

   Chcete-li protokolovat události návštěvy povoleného webu, je třeba také nakonfigurovat součást Kontrola webu (viz pokyny níže).

   V tabulce událostí můžete také povolit oznamování na obrazovce a oznamování e-mailem. Chcete-li odesílat upozornění e-mailem, musíte nakonfigurovat nastavení serveru SMTP. Další informace o zasílání upozornění e-mailem najdete v *nápovědě k aplikaci Kaspersky Security Center*.

6. Uložte změny.

Výsledkem je, že aplikace Kaspersky Endpoint Security začne protokolovat události aktivity uživatele na internetu.

Kontrola webu odešle události aktivity uživatelů do aplikace Kaspersky Security Center takto:

- Pokud používáte aplikaci Kaspersky Security Center, součást Kontrola webu odešle události pro všechny objekty, které tvoří webovou stránku. Z tohoto důvodu může být v případě, že je jeden web blokovaný, vytvořeno více událostí. Například při blokování webu http://www.priklad.cz může aplikace Kaspersky Endpoint Security předávat události pro následující objekty: http://www.priklad.cz, http://www.priklad.cz/ikona.ico, http://www.priklad.cz/soubor.js atd.

- Pokud používáte cloudovou konzolu aplikace Kaspersky Security Center, Kontrola webu seskupuje události a odesílá pouze protokol a doménu webu. Pokud například uživatel navštíví nedoporučené webové stránky http://www.priklad.cz/uvod, http://www.priklad.cz/kontakty a http://www.priklad.cz/galerie, aplikace Kaspersky Endpoint Security odešle pouze jednu událost s objektem http://www.priklad.cz.

Postup povolení protokolování událostí u návštěv povolených webů:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.

3. V bloku **Další** klikněte na tlačítko **Rozšířené nastavení**.

4. V okně, které se otevře, zaškrtněte políčko **Protokolovat otvírání povolených stránek**.

5. Uložte změny.

Díky tomu budete moci zobrazit celou historii prohlížeče.

Úprava šablon zpráv součásti Kontrola webu

V závislosti na typu akce zadané ve vlastnostech pravidel součásti Kontrola webu zobrazí aplikace Kaspersky Endpoint Security zprávu jednoho z následujících typů, když se uživatel pokusí o přístup k internetovým zdrojům (aplikace nahradí stránku HTML zprávou pro odpověď serveru HTTP):

- Varovná zpráva. Tato zpráva upozorňuje uživatele, že návštěva webového prostředku není doporučena a/nebo vede k porušení podnikových zásad zabezpečení. Aplikace Kaspersky Endpoint Security zobrazí varování, pokud

je v rozevíracím seznamu **Akce** v nastavení pravidla, které popisuje daný webový prostředek, vybrána položka **Varovat**.

Pokud se uživatel domnívá, že varování není opodstatněné, může kliknout na odkaz ve varování a odeslat předem vygenerovanou zprávu místnímu podnikovému správci sítě.

- Zpráva informující o blokování webového prostředku. Aplikace Kaspersky Endpoint Security zobrazí zprávu s informací, že webový prostředek je zablokován, pokud je možnost **Blokovat** vybrána v rozevíracím seznamu **Akce** v nastavení pravidla, které popisuje daný webový prostředek.

  Pokud se uživatel domnívá, že byl webový prostředek zablokován omylem, může kliknout na odkaz ve zprávě s upozorněním na zablokování webového prostředku a odeslat předem vygenerovanou zprávu místnímu podnikovému správci sítě.

Pro varovnou zprávu, zprávu s informací o zablokování webového prostředku a zprávu odesílanou správci sítě LAN jsou k dispozici zvláštní šablony. Jejich obsah můžete upravit.

Změna šablony pro zprávy součásti Kontrola webu:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola webu**.
3. V bloku **Šablony** nakonfigurujte šablony pro zprávy součásti Kontrola webu:
   - **Varování**. Pole pro zadání zahrnuje šablony zprávy, která se zobrazí, pokud je aktivováno pravidlo varování o pokusech o přístup k nežádoucímu webovému prostředku.
   - **Blokování**. Pole pro zadání obsahuje šablonu zprávy, která se zobrazí, pokud je aktivováno pravidlo, které blokuje přístup k webovému prostředku.
   - **Zpráva správci**. Pole pro zadání obsahuje šablonu zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem.
4. Uložte změny.

Úprava masek pro adresy webových prostředků

Použití *masky adresy webových prostředků* (také je označována jako „maska adresy“) může být užitečné, když při vytváření pravidla přístupu k webovým prostředkům potřebujete zadat řadu podobných adres webových prostředků. Dobře vytvořená maska adresy může nahradit velký počet adres webových prostředků.

Při vytváření masky adresy dodržujte tato pravidla:

1. Znak `*` nahrazuje jakoukoli sekvenci obsahující nula a více znaků.

   Pokud například zadáte masku adresy `*abc*`, pravidlo přístupu se použije na všechny webové prostředky, které obsahují sekvenci `abc`. Příklad: `http://www.priklad.cz/stranka_0-9abcdef.html`.

2. Posloupnost znaků `*.` (známá jako *maska domény*) vám umožní vybrat všechny domény adresy. Maska domény `*.` představuje libovolný název domény, název subdomény nebo prázdný řádek.

   Příklad: maska `*.priklad.cz` představuje následující adresy:

   - `http://fotky.priklad.cz`. Maska domény `*.` představuje `fotky.`
   - `http://uzivatel.fotky.priklad.cz`. Maska domény `*.` představuje `fotky.` a `uzivatel.`

- `http://priklad.cz`. Maska domény `*.` je interpretován jako prázdný řádek.

3. Sekvence znaků `www.` na začátku masky adresy je interpretována jako sekvence `*.`.

   Příklad: Maska adresy `www.priklad.cz` je zpracována jako `*.priklad.cz`. Tato maska pokrývá adresy `www2.priklad.cz` a `www.fotky.priklad.cz`.

4. Pokud maska adresy nezačíná znakem `*`, obsah masky adresy odpovídá stejnému obsahu s předponou (`*.`).

5. Pokud maska adresy končí jiným znakem než `/` nebo `*`, obsah masky adresy odpovídá stejnému obsahu s příponou `/*`.

   Příklad: Maska adresy `http://www.priklad.cz` zahrnuje adresy jako například `http://www.priklad.cz/abc`, kde znaky `a`, `b`, a `c` jsou libovolné znaky.

6. Pokud maska adresy končí znakem `/`, obsah masky adresy odpovídá stejnému obsahu s příponou `/*.`.

7. Sekvence znaků `/*` na konci masky adresy je interpretována jako `/*` nebo prázdný řetězec.

8. Adresy webových prostředků jsou ověřovány pomocí masky adresy a při této operaci je brán v potaz protokol (http nebo https):

   - Pokud maska adresy neobsahuje žádný síťový protokol, tato maska adresy zahrnuje adresy s jakýmkoli síťovým protokolem.

     Příklad: Maska adresy `priklad.cz` pokrývá adresy `http://priklad.cz` a `https://priklad.cz`.

   - Pokud maska adresy obsahuje nějaký síťový protokol, tato maska adresy zahrnuje jen adresy se stejným síťovým protokolem, který je v masce adresy.

     Příklad: Maska adresy `http://*.priklad.cz` zahrnuje adresu `http://www.priklad.cz`, ale nezahrnuje adresu `https://www.priklad.cz`.

9. Maska adresy, která je v dvojitých uvozovkách, je zpracována bez zohlednění jakýchkoli dalších nahrazení, kromě znaku `*`, pokud byl do masky adresy původně zahrnut. Pravidla 5 a 7 neplatí pro masky adresy uzavřené v dvojitých uvozovkách (viz příklady 14–18 v tabulce níže).

10. Uživatelské jméno a heslo, port připojení a velká a malá písmena nejsou při porovnávání s maskou adresy webového prostředku brány v potaz.

Příklady použití pravidel při vytváření masek adresy

Č.	Maska adresy	Adresa webového prostředku k ověření	Maska adresy danou adresu zahrnuje	Poznámka
1	*.priklad.com	http://www.123example.com	Ne	Viz pravidlo 1.
2	*.priklad.com	http://www.123.example.com	Ano	Viz pravidlo 2.
3	*priklad.com	http://www.123example.com	Ano	Viz pravidlo 1.
4	*priklad.com	http://www.123.example.com	Ano	Viz pravidlo 1.
5	http://www.*.example.com	http://www.123example.com	Ne	Viz pravidlo 1.
6	www.priklad.com	http://www.example.com	Ano	Viz pravidla 3, 2, 1.
7	www.priklad.com	https://www.example.com	Ano	Viz pravidla 3, 2, 1.

8	http://www.*.example.com	http://123.example.com	Ano	Viz pravidla 3, 4, 1.
9	www.priklad.com	http://www.example.com/abc	Ano	Viz pravidla 3, 5, 1.
10	priklad.com	http://www.example.com	Ano	Viz pravidly 3, 1.
11	http://example.com/	http://example.com/abc	Ano	Viz pravidla 1.
12	http://priklad.com/*	http://example.com	Ano	Viz pravidlo 7.
13	http://example.com	https://example.com	Ne	Viz pravidlo 8.
14	"priklad.com"	http://www.example.com	Ne	Viz pravidlo 9.
15	"http://www.priklad.com"	http://www.example.com/abc	Ne	Viz pravidlo 9.
16	"*.priklad.com"	http://www.example.com	Ano	Viz pravidly 1, 9.
17	"http://www.priklad.com/*"	http://www.example.com/abc	Ano	Viz pravidly 1, 9.
18	"www.priklad.com"	http://www.priklad.com; https://www.priklad.com	Ano	Viz pravidly 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Ne	Maska adresy obsahuje více informací než jen adresu webového prostředku.

Migrace pravidel přístupu k webovým prostředkům z předchozích verzí aplikace

V případě upgradu aplikace Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows nebo dřívější verze aplikace na aplikaci Kaspersky Endpoint Security pro systém Windows 11.6.0 jsou pravidla přístupu k webovým prostředkům založená na kategoriích obsahu webových prostředků přenesena následujícím způsobem:

- Pravidla přístupu k webovým prostředkům založená na jedné nebo více kategoriích obsahu webových prostředků ze seznamů „Chaty a fóra“, „Webový e-mail“ a „Sociální sítě“ budou přenesena do kategorie obsahu webových prostředků „Síťová komunikace“.
- Pravidla přístupu k webovým prostředkům založená na jedné nebo více kategoriích obsahu webových prostředků ze seznamů „Internetové obchody“ a „Platební systémy“ budou přenesena do kategorie obsahu webových prostředků „Internetoví prodejci, banky, platební systémy“.
- Pravidla přístupu k webovým prostředkům založená na kategorii obsahu webových prostředků „Hry“ budou přenesena do kategorie obsahu „Hry, loterie, sázky“.
- Pravidla přístupu k webovým prostředkům založená na kategorii obsahu webových prostředků „Hry pro prohlížeče“ budou přenesena do kategorie obsahu „Počítačové hry“.
- Pravidla přístupu k webovým prostředkům založená na kategoriích obsahu webových prostředků, které nejsou zahrnuty ve výše uvedeném seznamu, budou přeneseny beze změn.

Kontrola zařízení

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Kontrola zařízení spravuje přístup uživatelů k zařízením, která jsou nainstalována v počítači nebo jsou k němu připojena (například pevné disky, fotoaparáty nebo moduly Wi-Fi). Díky tomu můžete chránit počítač před nakažením, když jsou taková zařízení připojena, a zabránit ztrátě nebo úniku dat.

Úrovně přístupu k zařízení

Součást Kontrola zařízení řídí přístup na následujících úrovních:

- **Typ zařízení**. Například zařízení, vyměnitelné jednotky a jednotky CD/DVD.

  Přístup k zařízení můžete nakonfigurovat následujícím způsobem:

  - Povolit – .
  - Blokovat – .
  - Závisí na sběrnici připojení (kromě sítě Wi-Fi) – .
  - Blokovat s výjimkami (pouze Wi-Fi) – .

- **Sběrnice připojení**. *Sběrnice připojení* je rozhraní, které slouží k připojení zařízení k počítači (například rozhraní USB nebo FireWire). Můžete tedy omezit připojení všech zařízení, například přes port USB.

  Přístup k zařízení můžete nakonfigurovat následujícím způsobem:

  - Povolit – .
  - Blokovat – .

- **Důvěryhodná zařízení**. *Důvěryhodná zařízení* jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

  Důvěryhodná zařízení můžete přidat na základě následujících dat:

  - **Zařízení dle ID**. Každé zařízení má jedinečný identifikátor (ID hardwaru neboli HWID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Příklad ID zařízení: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Přidání zařízení podle ID je praktické, když chcete přidat několik konkrétních zařízení.
  - **Zařízení dle modelu**. Každé zařízení má ID dodavatele (VID) a ID produktu (PID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Šablona pro zadání VID a PID: `VID_1234&PID_5678`. Přidání zařízení podle modelu je praktické, pokud v organizaci používáte zařízení určitého modelu. Tímto způsobem můžete přidat všechna zařízení tohoto modelu.
  - **Zařízení dle masky ID**. Pokud používáte více zařízení s podobnými ID, můžete je přidat do seznamu důvěryhodných zařízení pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `WDC_C *`.
  - **Zařízení dle masky modelu**. Pokud používáte více zařízení s podobnými VID nebo PID (například zařízení od stejného výrobce), můžete přidat zařízení na seznam důvěryhodných pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `VID_05AC & PID_ *`.

Součást Kontrola zařízení reguluje přístup uživatele k zařízením pomocí *pravidel přístupu*. Součást Kontrola zařízení umožňuje také uložit události připojení/odpojení zařízení. Chcete-li uložit události, je třeba nakonfigurovat registraci událostí do zásady.

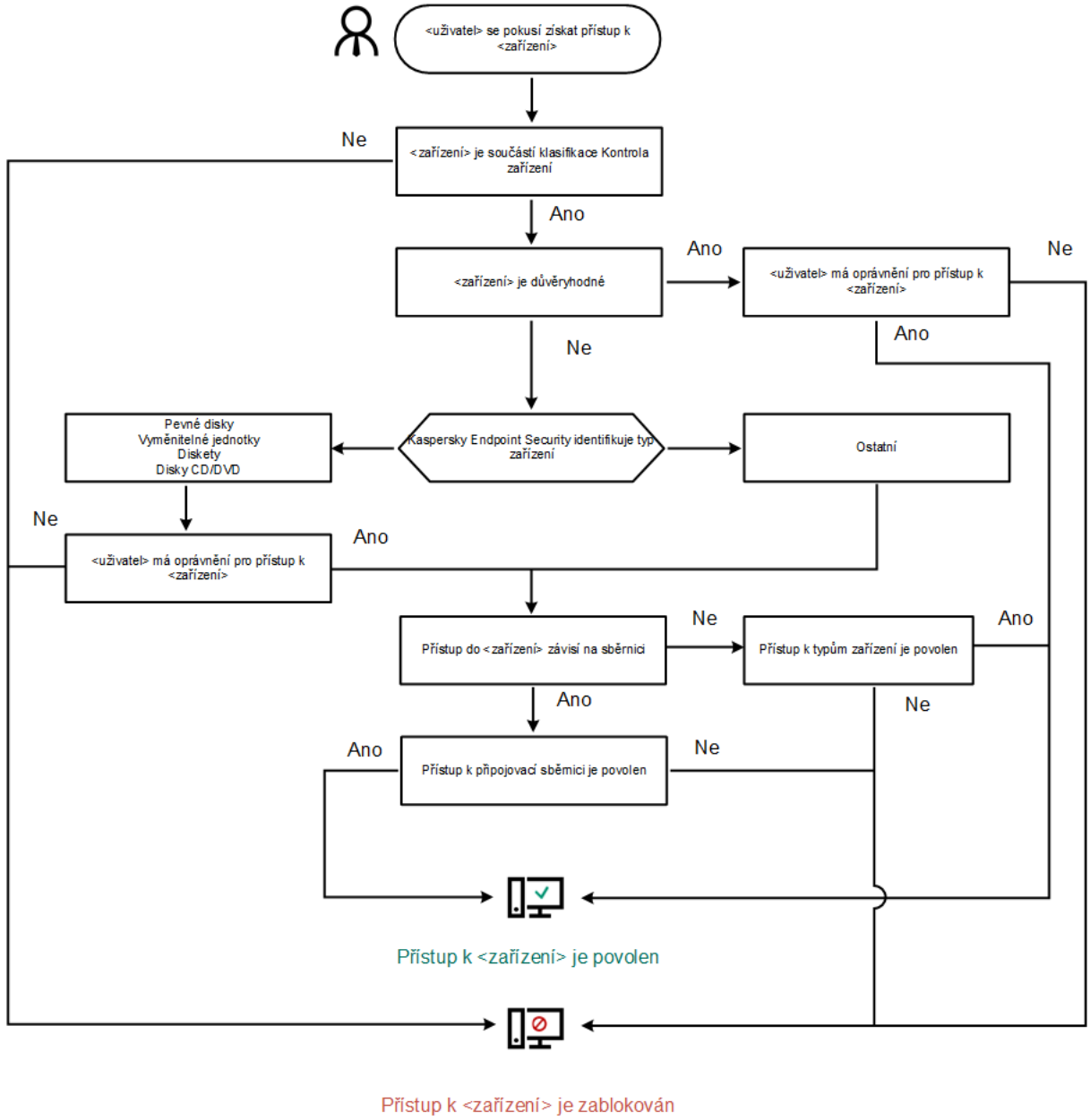
Pokud přístup k zařízení závisí na sběrnici připojení (stav), aplikace Kaspersky Endpoint Security neuloží události připojení/odpojení zařízení. Chcete-li aplikaci Kaspersky Endpoint Security umožnit, aby uložila události připojení/odpojení zařízení, povolte přístup k odpovídajícímu typu zařízení (stav) nebo přidejte zařízení do seznamu důvěryhodných zařízení.

Když je k počítači připojeno zařízení, které je blokováno součástí Kontrola zařízení, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).

Upozornění součásti Kontrola zařízení

Algoritmus činnosti součásti Kontrola zařízení

Aplikace Kaspersky Endpoint Security rozhoduje o tom, zda povolit přístup k zařízení poté, co ho uživatel připojí k počítači (viz obrázek níže).



Algoritmus činnosti součásti Kontrola zařízení

Pokud je zařízení připojeno a přístup je povolen, můžete upravit pravidlo přístupu a přístup blokovat. V takovém případě aplikace Kaspersky Endpoint Security při příštím pokusu o přístup k zařízení (například zobrazení stromu složek nebo provedení operace čtení nebo zápisu) zablokuje přístup. Zařízení bez souborového systému bude zablokováno až při příštím připojení zařízení.

Pokud musí uživatel počítače s nainstalovanou aplikací Kaspersky Endpoint Security zažádat o přístup k zařízení, o kterém si myslí, že je blokováno neopodstatněně, zašlete uživateli pokyny k vyžádání přístupu.

Povolení a zakázání součásti Kontrola zařízení

Součást Kontrola zařízení je ve výchozím nastavení povolena.

Postup povolení nebo zakázání součásti Kontrola zařízení:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

3. Pomocí přepínače **Kontrola zařízení** můžete tuto součást povolit nebo zakázat.

4. Uložte změny.

Pokud je součást Kontrola zařízení povolena, aplikace bude předávat informace o připojených zařízeních do aplikace Kaspersky Security Center. Seznam připojených zařízení můžete zobrazit v aplikaci Kaspersky Security Center ve složce **Hardware**.

O pravidlech přístupu

Pravidla přístupu obsahují skupinu nastavení, která určují, jací uživatelé mohou přistupovat k zařízením nainstalovaným v počítači nebo k němu připojeným. Nemůžete přidat zařízení, které je mimo klasifikaci součásti Kontrola zařízení. Přístup k takovým zařízením je povolen všem uživatelům.

Pravidla přístupu k zařízení

Skupina nastavení pravidla přístupu se liší v závislosti na typu zařízení (viz tabulka níže).

Nastavení pravidel přístupu

Zařízení	Řízení přístupu	Plán přístupu k zařízením	Přiřazení uživatelů nebo skupiny uživatelů	Priorita	Oprávnění ke čtení / k zápisu
Pevné disky	✓	✓	✓	✓	✓
Vyměnitelné jednotky	✓	✓	✓	✓	✓
Tiskárny	✓	–	–	–	–
Disketové jednotky	✓	✓	✓	✓	✓
Jednotky CD/DVD	✓	✓	✓	✓	✓
Modemy	✓	–	–	–	–
Pásková zařízení	✓	–	–	–	–
Multifunkční zařízení	✓	–	–	–	–
Čtečky čipových karet	✓	–	–	–	–
Zařízení USB ActiveSync se systémem Windows CE	✓	–	–	–	–
Adaptéry externí sítě	✓	–	–	–	–
Přenosná zařízení (MTP)	✓	✓	✓	✓	✓
Rozhraní Bluetooth	✓	–	–	–	–
Fotoaparáty a skenery	✓	–	–	–	–

Pravidla přístupu k mobilním zařízením

Mobilní zařízení se systémem Android nebo iOS jsou kategorizována jako přenosná zařízení (MTP). Pokud je k počítači připojeno mobilní zařízení, určuje typ zařízení operační systém. Pokud je v počítači nainstalován nástroj Android Debug Bridge (ADB), iTunes nebo obdobné aplikace, operační systém identifikuje mobilní zařízení jako zařízení ADB nebo iTunes. Ve všech ostatních případech může operační systém identifikovat typ mobilního zařízení jako přenosné zařízení (MTP) pro přenos souborů, zařízení PTP (fotoaparát) pro přenos obrazu nebo jiné zařízení. Typ zařízení závisí na modelu mobilního zařízení.

Vezměte na vědomí následující zvláštní aspekty týkající se přístupu k zařízením ADB nebo iTunes:

- Nelze nakonfigurovat plán přístupu k zařízením. Pokud je přístup k zařízením omezen pravidly (mají stav), zařízení ADB a iTunes jsou vždy přístupná.
- Nelze konfigurovat přístup zařízení pro jednotlivé uživatele ani konfigurovat přístupová oprávnění (čtení/zápis). Pokud je přístup k zařízením omezen pravidly (mají stav), zařízení ADB a iTunes jsou přístupná všem uživatelům se všemi oprávněními.
- Nelze nakonfigurovat přístup k důvěryhodným zařízením ADB ani iTunes pro jednotlivé uživatele. Pokud je zařízení důvěryhodné, zařízení ADB a iTunes jsou přístupná všem uživatelům.
- Pokud jste nainstalovali aplikace ADB nebo iTunes po připojení zařízení k počítači, může být resetováno jedinečné ID zařízení. To znamená, že aplikace Kaspersky Endpoint Security toto zařízení identifikuje jako nové zařízení. Pokud je zařízení důvěryhodné, přidejte jej znovu do seznamu důvěryhodných.

Pravidla přístupu udělují ve výchozím nastavení všem uživatelům úplný a nepřetržitý přístup k zařízením, pokud je povolen přístup ke sběrnicím připojení odpovídajících typů zařízení (stav).

Pravidla přístupu pro sítě Wi-Fi

Pravidlo přístupu pro síť Wi-Fi určuje, zda je povoleno (stav) nebo zakázáno (stav) použití sítí Wi-Fi. Můžete přidat *důvěryhodnou síť Wi-Fi* (stav) k pravidlu. Použití důvěryhodné sítě Wi-Fi je povoleno bez omezení. Ve výchozím nastavení umožňuje pravidlo přístupu pro síť Wi-Fi přístup k jakékoli síti Wi-Fi.

Pravidla přístupu ke sběrnici připojení

Pravidla přístupu ke sběrnici připojení určují, zda je povoleno (stav) nebo zakázáno (stav) připojení zařízení. Pravidla povolující přístup ke sběrnicím jsou ve výchozím nastavení vytvořena pro všechny sběrnice připojení přítomné v rámci klasifikace součásti Kontrola zařízení.

Úprava pravidla přístupu k zařízení

Pravidlo přístupu k zařízení je skupina nastavení, která určují, jak mohou uživatelé přistupovat k zařízením nainstalovaným v počítači nebo k němu připojeným. Mezi tato nastavení patří přístup ke konkrétnímu zařízení, plán přístupu a oprávnění ke čtení nebo zápisu.

Postup úpravy pravidla přístupu k zařízení:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Konfigurace přístupu** klikněte na tlačítko **Zařízení a Wi-Fi sítě**.

V okně, které se otevře, se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.

4. V bloku **Přístup k úložným zařízením** vyberte pravidlo přístupu, které chcete upravit. Blok obsahuje zařízení, která mají souborový systém, pro který můžete konfigurovat další nastavení přístupu. Pravidlo přístupu k zařízení uděluje ve výchozím nastavení všem uživatelům úplný přístup k zadanému typu zařízení bez omezení doby.

   a. V bloku **Přístup** vyberte příslušnou možnost přístupu k zařízení:

      - **Povolit**.
      - **Blokovat**.
      - **Závislé na sběrnici připojení**.

        Chcete-li zablokovat nebo povolit přístup k zařízení, nakonfigurujte přístup ke sběrnici připojení.
      - **Omezit pravidly**.

        Tato možnost umožňuje konfigurovat uživatelská práva, oprávnění a plán přístupu k zařízení.

   b. V části **Oprávnění uživatele** klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla přístupu k zařízení.

   c. Přiřaďte *pravidlu* prioritu. Pravidlo obsahuje následující atributy: uživatelský účet, plán, oprávnění (čtení/zápis) a priorita.

      Pravidlo má zvláštní prioritu. Pokud byl uživatel přidán do více skupin, řídí aplikace Kaspersky Endpoint Security přístup k zařízení na základě pravidla s nejvyšší prioritou. Kaspersky Endpoint Security vám umožňuje přiřadit prioritu od 0 do 10 000. Čím vyšší hodnota, tím vyšší priorita. Jinými slovy, položka s hodnotou 0 má nejnižší prioritu.

      Například můžete skupině Všichni udělit oprávnění jen pro čtení a skupině správců udělit oprávnění ke čtení a zápisu. Chcete-li tak učinit, přiřaďte skupině správců prioritu 1 a skupině Všichni prioritu 0.

      Priorita pravidla blokování je vyšší než priorita pravidla povolení. Jinými slovy, pokud byl uživatel přidán do více skupin a priorita všech pravidel je stejná, Kaspersky Endpoint Security řídí přístup k zařízení na základě jakéhokoli existujícího pravidla blokování.

   d. U pravidla přístupu k zařízení nastavte stav **Povoleno**.

   e. Nakonfigurujte přístupová oprávnění uživatele k zařízení: čtení a/nebo zápis.

   f. Vyberte uživatele nebo skupinu uživatelů, na které chcete použít pravidlo přístupu k zařízení.

   g. Nakonfigurujte plán přístupu k zařízení pro uživatele.

   h. Klikněte na tlačítko **Přidat**.

5. V bloku **Přístup k externím zařízením** vyberte pravidlo a nakonfigurujte přístup: **Povolit**, **Zamítnout** nebo **Závislé na sběrnici připojení**. V případě potřeby nakonfigurujte přístup ke sběrnici připojení.

6. V bloku **Přístup k Wi-Fi sítím** klikněte na odkaz **Wi-Fi** a nakonfigurujte přístup: **Povolit**, **Blokovat** nebo **Blokovat s výjimkami**. V případě potřeby přidejte Wi-Fi síť na seznam důvěryhodných.

7. Uložte změny.

Úprava pravidla přístupu ke sběrnici připojení

Postup úpravy pravidla přístupu ke sběrnici připojení:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Sběrnice připojení**.

   V okně, které se otevře, se zobrazují pravidla přístupu pro všechny sběrnice připojení, které jsou zahrnuty v klasifikaci součásti Kontrola zařízení.
4. Vyberte pravidlo přístupu, které chcete upravit.
5. Ve sloupci **Přístup** vyberte, zda chcete povolit přístup ke sběrnici připojení: **Povolit** nebo **Zamítnout**.
6. Uložte změny.

Přidání sítě Wi-Fi do seznamu důvěryhodných

Uživatelům můžete povolit připojování k sítím Wi-Fi, které považujete za bezpečné – například firemní síť Wi-Fi. Aby to bylo možné, musíte síť přidat na seznam důvěryhodných sítí Wi-Fi. Kontrola zařízení bude blokovat přístup ke všem sítím Wi-Fi s výjimkou těch určených v seznamu důvěryhodných.

Postup přidání sítě Wi-Fi do seznamu důvěryhodných:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu pro zařízení a Wi-Fi sítě**.

   V okně, které se otevře, se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.
4. V bloku **Přístup k Wi-Fi sítím** klikněte na odkaz **Wi-Fi**.

   V okně, které se otevře, se zobrazují pravidla přístupu k Wi-Fi síti.
5. Ve sloupci **Přístup** vyberte **Blokovat s výjimkami**.
6. V bloku **Důvěryhodná Wi-Fi síť** klikněte na tlačítko **Přidat**.
7. V okně, které se otevře, proveďte jednu z následujících akcí:

   a. V poli **Název sítě** zadejte název sítě Wi-Fi, kterou chcete přidat na seznam důvěryhodných.

   b. V rozevíracím seznamu **Typ ověřování** vyberte typ ověřování používaný při připojování k důvěryhodné síti Wi-Fi.

   c. V rozevíracím seznamu **Typ šifrování** vyberte typ šifrování používaný k zabezpečení provozu v rámci důvěryhodné sítě Wi-Fi.

d. Do pole **Poznámka** můžete zadat jakékoli informace o přidané síti Wi-Fi.

Síť Wi-Fi bude považována za důvěryhodnou, pokud se její nastavení budou shodovat se všemi nastaveními určenými v pravidle.

8. Uložte změny.

Monitorování využití vyměnitelných jednotek

Postup povolení monitorování využití vyměnitelné jednotky:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu pro zařízení a Wi-Fi sítě**.

   V okně, které se otevře, se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.
4. V bloku **Přístup k úložným zařízením** vyberte možnost **Vyměnitelné jednotky**.
5. Klikněte na odkaz **Protokolování**.
6. V okně, které se otevře, vyberte kartu **Protokolování**.
7. Zapněte přepínač **Protokolování**.
8. V bloku **Operace se soubory** vyberte operace, které chcete monitorovat: **zápis**, **odstranění**.
9. V bloku **Filtrovat podle formátů souborů** vyberte formáty souborů, jejichž přidružené operace by měla součást Kontrola zařízení monitorovat.
10. Vyberte uživatele nebo skupinu uživatelů, u nichž chcete používání vyměnitelných jednotek monitorovat.
11. Uložte změny.

Když uživatel provede zápis do souborů na vyměnitelných jednotkách nebo odstraní soubory z vyměnitelných jednotek, aplikace Kaspersky Endpoint Security uloží informace o těchto operacích do protokolu událostí a odešle zprávu do aplikace Kaspersky Security Center. Události spojené se soubory na vyměnitelných jednotkách můžete zobrazit v konzoli pro správu aplikace Kaspersky Security Center v pracovním prostoru uzlu **Administrační server** na kartě **Události**. Chcete-li zobrazit události v místním protokolu událostí aplikace Kaspersky Endpoint Security, je nutné zaškrtnout políčko **Byla provedena operace se souborem.** v nastavení upozornění pro součást Kontrola zařízení.

Změna doby ukládání do mezipamětintrol

Součást Kontrola zařízení eviduje události související se sledovanými zařízeními, jako je připojení a odpojení zařízení, čtení souboru ze zařízení, zápis souboru do zařízení, a další události. Kontrola zařízení poté povolí nebo zablokuje akci podle nastavení aplikace Kaspersky Endpoint Security.

Kontrola zařízení ukládá informace o událostech po určitou dobu, která se nazývá *doba ukládání do mezipaměti*. Pokud jsou informace o události uloženy do mezipaměti a tato událost se opakuje, není nutné o tom informovat aplikaci Kaspersky Endpoint Security ani zobrazovat další výzvu k udělení přístupu k příslušné akci, například připojení zařízení. Díky tomu je práce se zařízením pohodlnější.

Událost je považována za duplicitní událost, pokud všechna následující nastavení událostí odpovídají záznamu v mezipaměti:

- ID zařízení
- SID uživatelského účtu, který se pokouší o přístup
- Kategorie zařízení
- Akce provedená se zařízením
- Verdikt povolení aplikace pro tuto akci: povoleno nebo zamítnuto
- Cesta k procesu použitému k provedení akce
- Soubor, ke kterému se přistupuje

Před změnou doby ukládání do mezipaměti zakažte sebeobranu aplikace Kaspersky Endpoint Security. Po změně období ukládání do mezipaměti sebeobranu povolte.

Postup změny období ukládání do mezipaměti:

1. Otevřete editor registru v počítači.
2. V editoru registru přejděte do následující části:
   - Pro 64bitové operační systémy: [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]
   - Pro 32bitové operační systémy: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]
3. Otevřete DeviceControlEventsCachePeriod pro úpravy.
4. Definujte počet minut, po které má součást Kontrola zařízení ukládat informace o události, než budou tyto informace odstraněny.

Akce využívající důvěryhodná zařízení

Důvěryhodná zařízení jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

Chcete-li pracovat s důvěryhodnými zařízeními, můžete udělit přístup jednotlivému uživateli, skupině uživatelů nebo všem uživatelům organizace.

Pokud například vaše organizace nepovoluje použití vyměnitelných jednotek, ale správci je používají ve své práci, můžete vyměnitelné jednotky povolit pouze pro skupinu správců. Chcete-li tak učinit, přidejte vyměnitelné jednotky do seznamu důvěryhodných zařízení a nakonfigurujte přístupová oprávnění uživatelů.

Aplikace Kaspersky Endpoint Security umožňuje přidat zařízení do seznamu důvěryhodných zařízení následujícími způsoby:

- Pokud aplikace Kaspersky Security Center není ve vaší organizaci nasazena, můžete zařízení připojit k počítači a přidat jej do seznamu důvěryhodných zařízení v nastavení aplikace. Chcete-li distribuovat seznam důvěryhodných zařízení do všech počítačů ve vaší organizaci, můžete povolit slučování seznamů důvěryhodných zařízení nebo použít proces exportu/importu.

- Pokud je ve vaší organizaci nasazena aplikace Kaspersky Security Center, můžete vzdáleně detekovat všechna připojená zařízení a vytvořit v zásadách seznam důvěryhodných zařízení. Seznam důvěryhodných zařízení bude k dispozici na všech počítačích, na které se zásady vztahují.

Při práci s důvěryhodnými zařízeními má aplikace Kaspersky Endpoint Security následující omezení:

- Pluginy pro správu aplikace Kaspersky Endpoint Security verze 11.0.0–11.2.0 nemohou pracovat se seznamem důvěryhodných zařízení, který byl vytvořen v aplikaci Kaspersky Endpoint Security verze 11.3.0 a 11.4.0. Chcete-li pracovat se seznamem důvěryhodných zařízení z těchto verzí, je nutné upgradovat plugin pro správu na verzi 11.3.0 a 11.4.0.

- Pluginy pro správu aplikace Kaspersky Endpoint Security verze 11.3.0 a 11.4.0 nemohou pracovat se seznamem důvěryhodných zařízení, který byl vytvořen v aplikaci Kaspersky Endpoint Security verze 11.2.0 nebo starší. Aby tyto verze fungovaly se seznamem důvěryhodných zařízení, musí být aplikace upgradována na verzi 11.3.0, případně 11.4.0. Prostřednictvím portálu Kaspersky CompanyAccount můžete také zaslat požadavek obsahující popis vaší situace technické podpoře.

- Chcete-li migrovat seznam důvěryhodných zařízení z aplikace Kaspersky Endpoint Security verze 11.2.0 na verzi 11.3.0, pošlete požadavek obsahující popis vaší situace technické podpoře prostřednictvím portálu Kaspersky CompanyAccount.

Přidání zařízení na seznam důvěryhodných z rozhraní aplikace

Když je při výchozím nastavení přidáno zařízení na seznam důvěryhodných zařízení, přístup k tomuto zařízení bude udělen všem uživatelům (skupina uživatelů Všichni).

Postup přidání zařízení na seznam důvěryhodných z rozhraní aplikace:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

3. V bloku **Nastavení** klikněte na tlačítko **Důvěryhodná zařízení**.

   Otevře se seznam důvěryhodných zařízení.

4. Klikněte na tlačítko **Vybrat**.

   Otevře se seznam připojených zařízení. Seznam zařízení je závislý na hodnotě vybrané v rozevíracím seznamu **Zobrazit připojená zařízení**.

5. V seznamu zařízení vyberte zařízení, které chcete přidat na seznam důvěryhodných.

6. V poli **Poznámka** můžete uvést jakékoli relevantní informace o důvěryhodném zařízení.

7. Vyberte uživatele nebo skupinu uživatelů, kterým chcete povolit přístup k důvěryhodným zařízením.

8. Uložte změny.

Přidání zařízení na seznam důvěryhodných z rozhraní aplikace Kaspersky Security Center

Aplikace Kaspersky Security Center přijímá informace o zařízeních, pokud je v počítačích nainstalován produkt Kaspersky Endpoint Security a je povolena součást Kontrola zařízení. Zařízení nelze přidat na seznam důvěryhodných zařízení, pokud informace o tomto zařízení nejsou k dispozici v aplikaci Kaspersky Security Center.

Zařízení můžete na seznam důvěryhodných zařízení přidat podle následujících údajů:

- **Zařízení dle ID**. Každé zařízení má jedinečný identifikátor (ID hardwaru neboli HWID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Příklad ID zařízení: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Přidání zařízení podle ID je praktické, když chcete přidat několik konkrétních zařízení.

- **Zařízení dle modelu**. Každé zařízení má ID dodavatele (VID) a ID produktu (PID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Šablona pro zadání VID a PID: `VID_1234&PID_5678`. Přidání zařízení podle modelu je praktické, pokud v organizaci používáte zařízení určitého modelu. Tímto způsobem můžete přidat všechna zařízení tohoto modelu.

- **Zařízení dle masky ID**. Pokud používáte více zařízení s podobnými ID, můžete je přidat do seznamu důvěryhodných zařízení pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `WDC_C *`.

- **Zařízení dle masky modelu**. Pokud používáte více zařízení s podobnými VID nebo PID (například zařízení od stejného výrobce), můžete přidat zařízení na seznam důvěryhodných pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `VID_05AC & PID_ *`.

Postup přidání zařízení na seznam důvěryhodných zařízení:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V okně zásad vyberte možnost **Kontrolní prvky zabezpečení → Kontrola zařízení**.

6. V pravé části okna vyberte kartu **Důvěryhodná zařízení**.

7. Pokud chcete vytvořit konsolidovaný seznam důvěryhodných zařízení pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**.

   Seznamy důvěryhodných zařízení v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Důvěryhodná zařízení z nadřazené zásadě se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna nebo odstranění důvěryhodných zařízení v nadřazené zásadě nejsou možné.

8. Klikněte na tlačítko **Přidat** a vyberte způsob přidání zařízení na seznam důvěryhodných zařízení.

9. Chcete-li filtrovat zařízení, vyberte typ zařízení z rozevíracího seznamu **Typ zařízení** (například **Vyměnitelné jednotky**).

10. Do pole **Název/model** zadejte ID, model (VID a PID) nebo masku zařízení, v závislosti na vybraném způsobu přidání.

    Přidání zařízení podle masky modelu (VID a PID) funguje takto: pokud zadáte masku modelu, která neodpovídá žádnému modelu, aplikace Kaspersky Endpoint Security zkontroluje, zda se ID zařízení (HWID) shoduje s maskou. Aplikace Kaspersky Endpoint Security kontroluje pouze část ID zařízení, která určuje výrobce a typ zařízení (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Pokud se maska modelu shoduje s touto částí ID zařízení, zařízení, která se shodují s maskou, budou přidána do seznamu důvěryhodných zařízení v počítači. Seznam zařízení v aplikaci Kaspersky Security Center současně zůstane po kliknutí na tlačítko **Obnovit** prázdný. Chcete-li zobrazit seznam zařízení správně, můžete přidat zařízení podle masky ID zařízení.

11. Chcete-li filtrovat zařízení, do pole **Počítač** zadejte název počítače nebo masku názvu počítače, ke kterému je zařízení připojeno.

    Znak `*` nahrazuje jakoukoli sadu znaků. Znak `?` nahrazuje jakýkoli jeden znak.

12. Klikněte na tlačítko **Aktualizovat**.

    V tabulce se zobrazuje seznam zařízení, která splňují definovaná kritéria filtrování.

13. Zaškrtněte políčko u názvů zařízení, které chcete přidat na seznam důvěryhodných zařízení.

14. Do pole **Poznámka** zadejte popis důvodu přidání zařízení na seznam důvěryhodných zařízení.

15. Klikněte na tlačítko **Vybrat** vpravo od pole **Povolit uživatelům a/nebo skupinám uživatelů**.

16. Vyberte uživatele nebo skupinu ve službě Active Directory a potvrďte výběr.

    Ve výchozím nastavení je přístup k důvěryhodným zařízením povolen pro skupinu Všichni.

17. Uložte změny.

Po připojení zařízení zkontroluje aplikace Kaspersky Endpoint Security seznam důvěryhodných zařízení pro oprávněného uživatele. Je-li zařízení důvěryhodné, aplikace Kaspersky Endpoint Security umožní přístup k zařízení se všemi oprávněními, i když je přístup k typu zařízení nebo připojovací sběrnici odepřen. Pokud je zařízení nedůvěryhodné a přístup byl odepřen, můžete požádat o přístup k uzamknutému zařízení.

Export a import seznamu důvěryhodných zařízení

Chcete-li distribuovat seznam důvěryhodných zařízení do všech počítačů ve vaší organizaci, můžete použít proces exportu/importu.

Pokud například potřebujete distribuovat seznam důvěryhodných vyměnitelných jednotek, musíte provést následující kroky:

1. Postupně připojujte vyměnitelné jednotky k počítači.

2. V nastavení aplikace Kaspersky Endpoint Security přidejte vyměnitelné jednotky na seznam důvěryhodných zařízení. V případě potřeby nakonfigurujte oprávnění přístupu uživatelů. Povolte například přístup

k vyměnitelným jednotkám pouze správcům.

3. V nastavení aplikace Kaspersky Endpoint Security exportujte seznam důvěryhodných zařízení (viz pokyny níže).

4. Distribuujte soubor seznamu důvěryhodných zařízení do jiných počítačů ve vaší organizaci. Soubor umístěte například do sdílené složky.

5. V nastavení aplikace Kaspersky Endpoint Security importujte seznam důvěryhodných zařízení do jiných počítačů v organizaci (viz pokyny níže).

Potup importu nebo exportu seznamu důvěryhodných zařízení:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

3. V bloku **Nastavení** klikněte na tlačítko **Důvěryhodná zařízení**.

   Otevře se seznam důvěryhodných zařízení.

4. Potup exportu seznamu důvěryhodných zařízení:

   a. Vyberte důvěryhodná zařízení, která chcete exportovat.

   b. Klikněte na tlačítko **Exportovat**.

   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam důvěryhodných zařízení, a vyberte složku, do které chcete tento soubor uložit.

   d. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam důvěryhodných zařízení do souboru XML.

5. Postup importu seznamu důvěryhodných zařízení:

   a. V rozevíracím seznamu **Importovat** vyberte příslušnou akci: **Importovat a přidat mezi stávající** nebo **Importovat a nahradit stávající**.

   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam důvěryhodných zařízení.

   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam důvěryhodných zařízení obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

6. Uložte změny.

Po připojení zařízení zkontroluje aplikace Kaspersky Endpoint Security seznam důvěryhodných zařízení pro oprávněného uživatele. Je-li zařízení důvěryhodné, aplikace Kaspersky Endpoint Security umožní přístup k zařízení se všemi oprávněními, i když je přístup k typu zařízení nebo připojovací sběrnici odepřen.

Získání přístupu k blokovanému zařízení

Při konfiguraci součásti Kontrola zařízení můžete náhodně zablokovat přístup k zařízení, které je nezbytné pro práci.

Pokud aplikace Kaspersky Security Center není ve vaší organizaci nasazena, můžete poskytnout přístup k zařízení v nastavení aplikace Kaspersky Endpoint Security. Můžete například přidat zařízení na seznam důvěryhodných zařízení nebo dočasně zakázat součást Kontrola zařízení.

Pokud je aplikace Kaspersky Security Center ve vaší organizaci nasazena a na počítače byly použity zásady, můžete poskytnout přístup k zařízení v konzole pro správu.

Online režim pro udělení přístupu

Přístup k blokovanému zařízení můžete udělit v režimu online pouze v případě, že je v organizaci nasazena aplikace Kaspersky Security Center a na počítač se uplatňují zásady. Počítač musí mít možnost navázat spojení se serverem pro správu.

Udělení přístupu v režimu online se skládá z následujících kroků:

1. Uživatel odešle správci zprávu obsahující požadavek na přístup.
2. Správce přidá zařízení do seznamu důvěryhodných zařízení.

   Důvěryhodné zařízení můžete přidat v zásadách pro skupinu pro správu nebo v místním nastavení aplikace pro jednotlivý počítač.
3. Správce aktualizuje nastavení aplikace Kaspersky Endpoint Security v počítači uživatele.

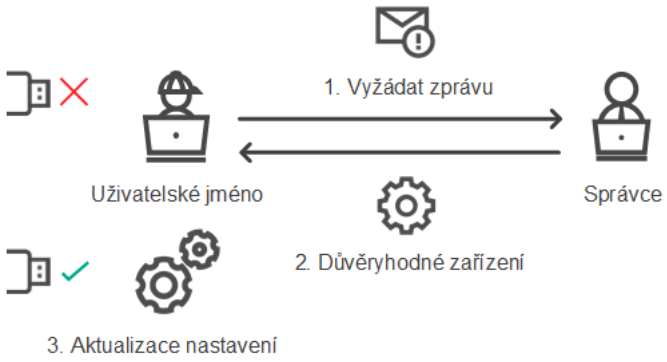


Schéma pro udělení přístupu k zařízení v režimu online

Offline režim pro udělení přístupu

Přístup k blokovanému zařízení můžete udělit v režimu offline pouze v případě, že je v organizaci nasazena aplikace Kaspersky Security Center a na počítač se uplatňují zásady. V nastavení zásad v části **Kontrola zařízení** musí být zaškrtnuto políčko **Povolit žádosti o dočasný přístup**.

Pokud potřebujete udělit dočasný přístup k blokovanému zařízení, ale nemůžete je přiat na seznam důvěryhodných zařízení, můžete k zařízení udělit přístup v režimu offline. Tímto způsobem můžete udělit přístup k blokovanému zařízení i v případě, že počítač nemá přístup k síti nebo je mimo podnikovou síť.

Udělení přístupu v režimu offline se skládá z následujících kroků:

1. Uživatel vytvoří soubor se žádostí o přístup a odešle jej správci.
2. Správce ze souboru se žádostí o přístup vytvoří přístupový klíč a odešle jej uživateli.

3. Uživatel aktivuje přístupový klíč.

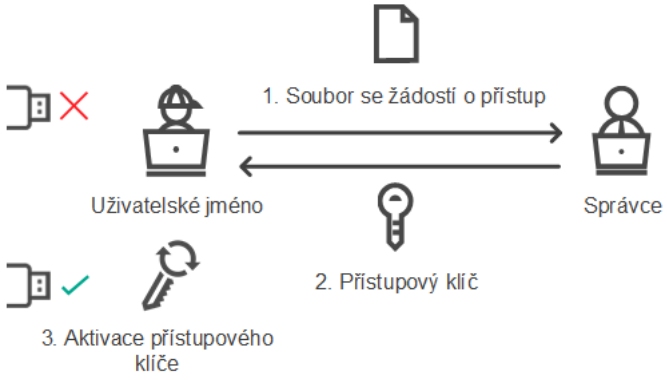


Schéma pro udělení přístupu k zařízení v režimu offline

Online režim pro udělení přístupu

Přístup k blokovanému zařízení můžete udělit v režimu online pouze v případě, že je v organizaci nasazena aplikace Kaspersky Security Center a na počítač se uplatňují zásady. Počítač musí mít možnost navázat spojení se serverem pro správu.

Uživatel požádá o přístup k blokovanému zařízení takto:

1. Připojte zařízení k počítači.

   Aplikace Kaspersky Endpoint Security zobrazí upozornění, že přístup k zařízení je blokován (viz obrázek níže).

2. Klikněte na odkaz **Požádat o přístup**.

   Otevře se okno **Zpráva správce**. Tato zpráva obsahuje informace o blokovaném zařízení.

3. Klikněte na tlačítko **Odeslat**.

Správce obdrží zprávu obsahující žádost o poskytnutí přístupu, například e-mailem. Další podrobnosti o zpracování požadavků uživatelů naleznete v *nápovědě k aplikaci Kaspersky Security Center*. Po přidání zařízení na seznam důvěryhodných zařízení a aktualizaci nastavení aplikace Kaspersky Endpoint Security v počítači uživatel získá přístup k zařízení.

Upozornění součásti Kontrola zařízení

Offline režim pro udělení přístupu

Přístup k blokovanému zařízení můžete udělit v režimu offline pouze v případě, že je v organizaci nasazena aplikace Kaspersky Security Center a na počítač se uplatňují zásady. V nastavení zásad v části **Kontrola zařízení** musí být zaškrtnuto políčko **Povolit žádosti o dočasný přístup**.

Uživatel požádá o přístup k blokovanému zařízení takto:

1. Připojte zařízení k počítači.

   Aplikace Kaspersky Endpoint Security zobrazí upozornění, že přístup k zařízení je blokován (viz obrázek níže).

2. Klikněte na odkaz **Požádat o dočasný přístup**.

   Otevře se okno **Požádat o přístup k zařízení** se seznamem připojených zařízení.

3. V seznamu připojených zařízení vyberte to, ke kterému chcete získat přístup.

4. Klikněte na tlačítko **Vytvořit soubor se žádostí o přístup**.

5. Do pole **Délka přístupu** zadejte časové období, během kterého chcete mít přístup k zařízení.

6. Uložte soubor do paměti počítače.

Soubor se žádostí o přístup s příponou*.akey bude stažen do paměti počítače. Libovolným dostupným způsobem odešlete soubor se žádostí o přístup k zařízení správci podnikové sítě LAN.

Upozornění součásti Kontrola zařízení

Správce následujícím postupem vytvoří přístupový klíč pro blokované zařízení:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušný klientský počítač.

3. V pracovním prostoru vyberte kartu **Devices**.

4. V seznamu klientských počítačů vyberte počítač uživatele, který potřebuje získat dočasný přístup k uzamčenému zařízení.

5. V kontextové nabídce počítače vyberte položku **Udělit přístup v offline režimu**.

6. V okně, které se otevře, vyberte kartu **Kontrola zařízení**.

7. Klikněte na tlačítko **Procházet** a stáhněte soubor se žádostí o přístup přijatý od uživatele.

   Zobrazí se informace o blokovaném zařízení, ke kterému uživatel žádá o přístup.

8. V případě potřeby změňte hodnotu nastavení **Délka přístupu**.

   Ve výchozím nastavení **Délka přístupu** přebírá hodnotu udanou uživatelem při vytváření souboru se žádostí o přístup.

9. Zadejte hodnotu nastavení **Aktivuje**.

   Toto nastavení určuje časové období, během kterého může uživatel aktivovat přístup k zablokovanému zařízení pomocí poskytnutého přístupového klíče.

10. Uložte soubor s přístupovým klíčem do paměti počítače.

    Do paměti počítače se tak stáhne přístupový klíč pro blokované zařízení. Soubor s přístupovým klíčem má příponu*.acode. Libovolným způsobem zašlete přístupový klíč k blokovanému zařízení uživateli.

Uživatel aktivuje přístupový klíč následovně:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

3. V bloku **Žádost o přístup** klikněte na tlačítko **Požádat o přístup k zařízení**.

4. V okně, které se otevře, klikněte na tlačítko **Aktivovat přístupový klíč**.

5. V okně, které se otevře, vyberte soubor s přístupovým klíčem k zařízení přijatý od správce podnikové sítě LAN. Klikněte na tlačítko **Otevřít**.

   Otevře se okno obsahující informace o poskytnutí přístupu.

6. Klikněte na tlačítko **OK**.

   Uživatel získá přístup k zařízení po dobu stanovenou správcem. Uživatel obdrží úplný soubor práv pro přístup k zařízení (čtení a zápis). Po skončení platnosti klíče bude přístup k zařízení zablokován. Pokud uživatel vyžaduje trvalý přístup k zařízení, přidejte zařízení na seznam důvěryhodných zařízení.

Úprava šablon zpráv součásti Kontrola zařízení

Když se uživatel pokusí o přístup k blokovanému zařízení, aplikace Kaspersky Endpoint Security zobrazí zprávu s upozorněním na zablokování přístupu k danému zařízení nebo zakázání použití obsahu zařízení. Pokud se uživatel domnívá, že přístup k zařízení byl zablokován omylem nebo že použití obsahu zařízení bylo zakázáno nedopatřením, kliknutím na odkaz v zobrazené zprávě o zablokované akci může odeslat zprávu místnímu podnikovému správci sítě.

Pro zprávy o zablokovaném přístupu k zařízením nebo zakázaných akcích pro obsah zařízení a pro zprávu odesílanou správci jsou k dispozici šablony. Tyto šablony zpráv můžete upravit.

Postup úpravy šablon pro zprávy součásti Kontrola zařízení:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

3. V bloku **Šablony** nakonfigurujte šablony pro zprávy součásti Kontrola zařízení:

   - **Zpráva o blokování**. Šablona zprávy, která se zobrazí, když se uživatel pokusí o přístup k blokovanému zařízení. Tato zpráva se také zobrazí, když se uživatel pokusí provést činnost s obsahem zařízení, které bylo pro tohoto uživatele zablokováno.

   - **Zpráva správci**. Šablona zprávy, která bude odeslána správci sítě LAN, když se uživatel domnívá, že přístup k zařízení byl zablokován omylem nebo že činnosti s obsahem zařízení jsou nedopatřením zakázány.

4. Uložte změny.

Anti-Bridging

Anti-Bridging zamezuje vytváření síťových mostů tím, že brání tomu, aby se v počítači současně vytvářelo více síťových připojení. To vám umožní chránit podnikovou síť před útoky přes nechráněné nepovolané sítě.

Anti-Bridging reguluje vytváření síťových připojení pomocí *pravidel připojení*.

Pravidla připojení jsou vytvořena pro následující předdefinované typy zařízení:

- Síťové adaptéry
- Adaptéry Wi-Fi
- Modemy

V případě povolení pravidla připojení bude aplikace Kaspersky Endpoint Security provádět následující akce:

- Bude blokovat aktivní připojení během vytvoření nového připojení, pokud je typ zařízení určený v pravidlu používán pro obě připojení.
- Bude blokovat připojení navazovaná pomocí typů zařízení, pro které jsou používána pravidla nižší priority.

Povolení součásti Anti-Bridging

Součást Anti-Bridging je ve výchozím nastavení vypnuta.

Postup povolení součásti Anti-Bridging:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Anti-Bridging**.
4. Chcete-li povolit nebo zakázat tuto funkci, použijte přepínač **Povolit součást Anti-Bridging**.
5. Uložte změny.

Po povolení součásti Anti-Bridging aplikace Kaspersky Endpoint Security zablokuje již vytvořená připojení podle pravidel připojení.

Změna stavu pravidla připojení

Postup změny stavu pravidla připojení:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Anti-Bridging**.
4. V bloku **Pravidla pro zařízení** vyberte pravidlo, jehož stav chcete změnit.
5. Pomocí přepínačů ve sloupci **Kontrola** pravidlo povolíte nebo zakážete.
6. Uložte změny.

Změna priority pravidla připojení

Postup změny priority pravidla připojení:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení** klikněte na tlačítko **Anti-Bridging**.
4. V bloku **Pravidla pro zařízení** vyberte pravidlo, jehož prioritu chcete změnit.
5. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla připojení.

   Čím výše se pravidlo v tabulce pravidel nachází, tím vyšší je jeho priorita. Součást Anti-Bridging blokuje všechna připojení, kromě jednoho připojení navázaného pomocí typu zařízení, pro které je použito pravidlo nejvyšší priority.
6. Uložte změny.

Adaptivní kontrola anomálií

Tato součást je k dispozici pouze pro aplikace Kaspersky Endpoint Security for Business Advanced a Kaspersky Total Security for Business. Podrobnější informace o aplikaci Kaspersky Endpoint Security for Business najdete na *webu společnosti Kaspersky*.

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Adaptivní kontrola anomálií sleduje a blokuje akce, které nejsou obvyklé pro počítače v podnikové síti. Adaptivní kontrola anomálií používá ke sledování necharakteristického chování sadu pravidel (například pravidlo *Spuštění prostředí Microsoft PowerShell z aplikace sady Office*). Pravidla vytvářejí odborníci společnosti Kaspersky na základě typických scénářů škodlivé činnosti. Můžete nakonfigurovat, jak součást Adaptivní kontrola anomálií zpracovává každé pravidlo, a povolit například provádění skriptů PowerShell, které automatizují určité úlohy pracovního postupu. Aplikace Kaspersky Endpoint Security aktualizuje sadu pravidel spolu s databázemi aplikací. Aktualizace sad pravidel musí být potvrzeny ručně.

Nastavení součásti Adaptivní kontrola anomálií

Konfigurace součásti Adaptivní kontrola anomálií se skládá z následujících kroků:

1. Zkušební režim součásti Adaptivní kontrola anomálií.

   Poté, co povolíte součást Adaptivní kontrola anomálií, její pravidla fungují ve *zkušebním režimu*. Ve zkušebního režimu monitoruje součást Adaptivní kontrola anomálií aktivaci pravidel a odesílá aktivační události do centra Kaspersky Security Center. Každé pravidlo má své vlastní trvání zkušebního režimu. Doba trvání zkušebního režimu je nastavena odborníky společnosti Kaspersky. Obvykle je zkušební režim aktivní dva týdny.

   Pokud není během zkušebního režimu nějaké pravidlo aktivováno vůbec, bude součást Adaptivní kontrola anomálií akce spojené s tímto pravidlem považovat za netypické. Aplikace Kaspersky Endpoint Security bude blokovat všechny akce spojené s tímto pravidlem.

   Pokud bylo během zkušebního režimu nějaké pravidlo aktivováno, aplikace Kaspersky Endpoint Security zaznamená události do protokolu zpráva o aktivaci pravidel a úložiště **aktivace pravidel v chytrém zkušebním režimu**.

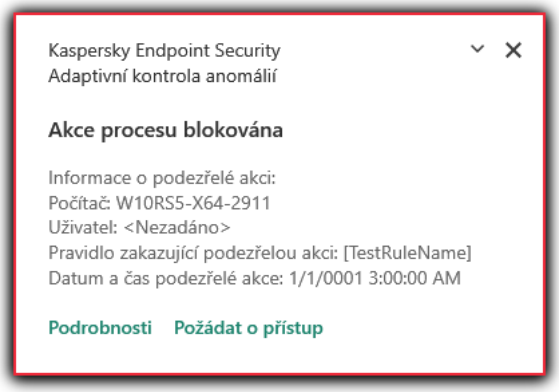
2. Analýza zprávy o aktivaci pravidel.

   Správce analyzuje zprávu o aktivaci pravidel nebo obsah úložiště **aktivace pravidel v chytrém zkušebním režimu**. Poté může správce zvolit chování součásti Adaptivní kontrola anomálií při aktivaci pravidla: blokovat nebo povolit. Správce může také sledovat, jak pravidlo funguje, a prodloužit dobu trvání zkušebního režimu. Pokud správce neprovede žádnou akci, aplikace bude i nadále fungovat ve zkušebním režimu. Doba zkušebního režimu začne běžet znovu.

Součást Adaptivní kontrola anomálií je konfigurována v reálném čase. Součást Adaptivní kontrola anomálií je konfigurována prostřednictvím následujících kanálů:

- Adaptivní kontrola anomálií automaticky začne blokovat akce spojené s pravidly, která nebyla nikdy spuštěna ve zkušebním režimu.
- Aplikace Kaspersky Endpoint Security přidává nová pravidla nebo odstraňuje zastaralá pravidla.
- Správce konfiguruje činnost součásti Adaptivní kontrola anomálií po kontrole zprávy o aktivaci pravidel a obsahu úložiště **aktivace pravidel v chytrém zkušebním režimu**. Doporučujeme zprávu o aktivaci pravidel a obsah úložiště **aktivace pravidel v chytrém zkušebním režimu kontrolovat**.

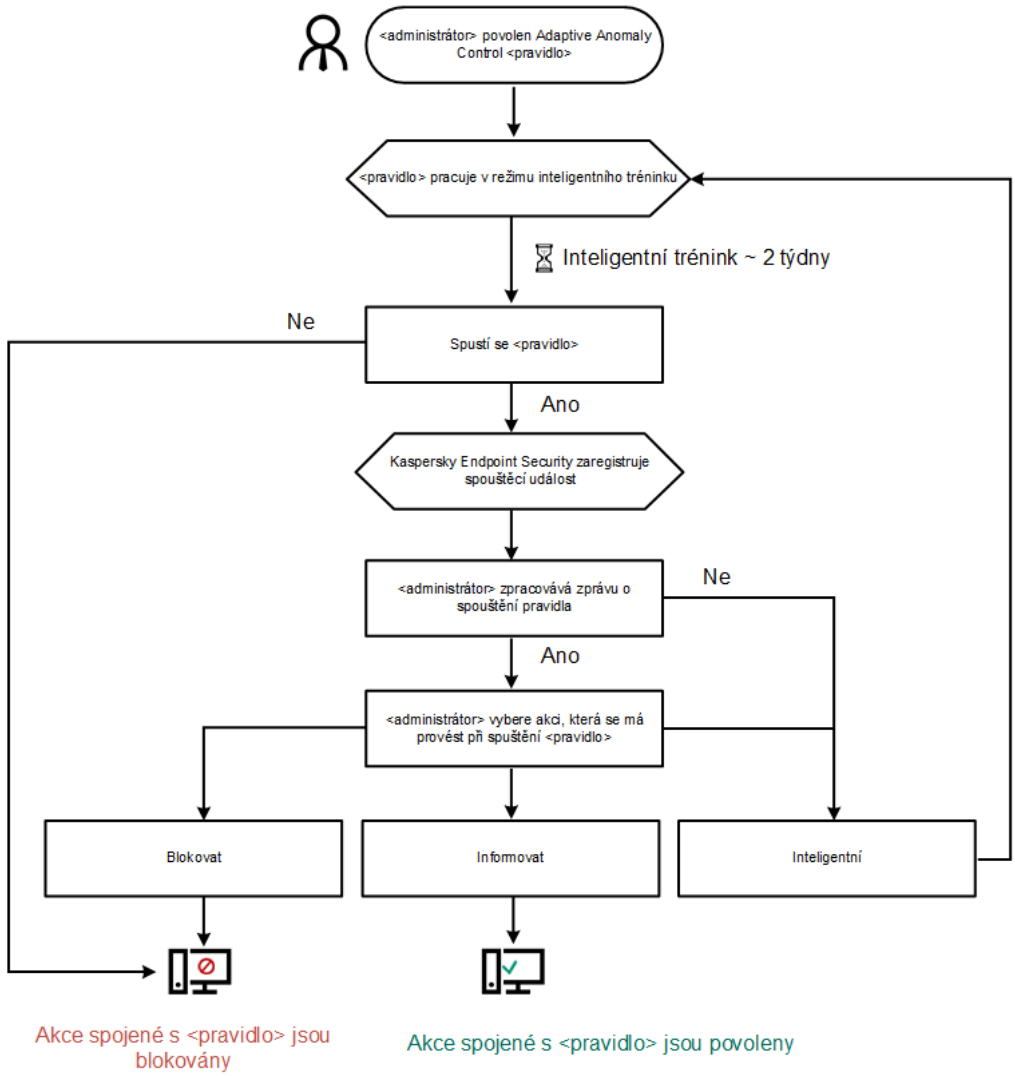
Pokud se škodlivá aplikace pokusí provést akci, aplikace Kaspersky Endpoint Security akci zablokuje a zobrazí upozornění (viz obrázek níže).



Oznámení součásti Adaptivní kontrola anomálií

Algoritmus činnosti součásti Adaptivní kontrola anomálií

Aplikace Kaspersky Endpoint Security určí, zda povolit nebo blokovat akci spojenou s pravidlem, na základě následujícího algoritmu (viz obrázek níže).



Algoritmus činnosti součásti Adaptivní kontrola anomálií

Povolení a zakázání součásti Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií je ve výchozím nastavení povolena.

Postup povolení nebo zakázání součásti Adaptivní kontrola anomálií:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.
3. Pomocí přepínače **Adaptivní kontrola anomálií** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Povolení a zakázání pravidla součásti Adaptivní kontrola anomálií

Postup povolení a zakázání pravidla součásti Adaptivní kontrola anomálií:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.
3. V bloku **Pravidla** klikněte na tlačítko **Upravit pravidla**.

   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií.
4. V tabulce vyberte sadu pravidel (například *Aktivita aplikací sady Office*) a sadu rozbalte.
5. Vyberte pravidlo (například spusťte *z aplikací Office Windows PowerShell*).
6. Pomocí přepínače ve sloupci **Stav** pravidlo součásti Adaptivní kontrola anomálií povolíte nebo zakážete.
7. Uložte změny.

Úprava akce provedené při spuštění pravidla součásti Adaptivní kontrola anomálií

Postup úprava akce, která se provede při spuštění pravidla součásti Adaptivní kontrola anomálií:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.
3. V bloku **Pravidla** klikněte na tlačítko **Upravit pravidla**.

   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií.
4. V tabulce vyberte pravidlo.
5. Klikněte na tlačítko **Upravit**.

Otevře se okno pravidel součásti Adaptivní kontrola anomálií.

6. V bloku **Akce** vyberte některou z následujících možností:

   - **Inteligentní**. Pokud je vybrána tato možnost, pravidlo součásti Adaptivní kontrola anomálií funguje v chytrém zkušebním režimu po dobu, která je definována odborníky společnosti Kaspersky. Pokud je v tomto režimu spuštěno pravidlo součásti Adaptivní kontrola anomálií, aplikace Kaspersky Endpoint Security povolí aktivitu, které se pravidlo týká, a vytvoří položku protokolu v úložišti pro **spuštění pravidel v chytrém zkušebním režimu** administračního serveru Kaspersky Security Center. Po skončení časového období nastaveného pro práci v chytrém zkušebním režimu aplikace Kaspersky Endpoint Security blokuje aktivitu, které se týká pravidlo součásti Adaptivní kontrola anomálií, a vytvoří položku protokolu obsahující informace o aktivitě.

   - **Blokovat**. Pokud je vybrána tato akce, při spuštění pravidla součásti Adaptivní kontrola anomálií aplikace Kaspersky Endpoint Security blokuje aktivitu, které se pravidlo týká, a vytvoří položku protokolu obsahující informace o aktivitě.

   - **Informovat**. Pokud je vybrána tato akce, při spuštění pravidla součásti Adaptivní kontrola anomálií aplikace Kaspersky Endpoint Security povolí aktivitu, které se pravidlo týká, a vytvoří položku protokolu obsahující informace o aktivitě.

7. Uložte změny.

Vytvoření výjimky pro pravidlo součásti Adaptivní kontrola anomálií

Nelze vytvořit více než1 000 výjimek pro pravidla součásti Adaptivní kontrola anomálií. Nedoporučuje se vytvářet více než 200 výjimek. Chcete-li snížit počet použitých výjimek, doporučuje se v nastaveních výjimek použít masky.

Výjimka pro pravidlo součásti Adaptivní kontrola anomálií obsahuje popis zdrojového a cílového objektu. *Zdrojový objekt* je objekt provádějící akce. *Cílový objekt* je objekt, na které jsou akce prováděny. Například jste otevřeli soubor s názvem `file.xlsx`. V důsledku toho je do paměti počítače načten soubor knihovny s příponou DLL. Tato knihovna je použita prohlížečem (spustitelný soubor s názvem `browser.exe`). V tomto příkladu je `file.xlsx` zdrojový objekt, Excel je zdrojový proces, `browser.exe` je cílový objekt a prohlížeč je cílový proces.

Vytvoření výjimky pro pravidlo součásti Adaptivní kontrola anomálií:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Adaptivní kontrola anomálií**.

3. V bloku **Pravidla** klikněte na tlačítko **Upravit pravidla**.

   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií.

4. V tabulce vyberte pravidlo.

5. Klikněte na tlačítko **Upravit**.

   Otevře se okno pravidel součásti Adaptivní kontrola anomálií.

6. V bloku **Výjimky** klikněte na tlačítko **Přidat**.

   Otevře se okno vlastností výjimky.

7. Vyberte uživatele, pro kterého chcete nakonfigurovat výjimku.

   Adaptivní kontrola anomálií nepodporuje výjimky pro skupiny uživatelů. Pokud vyberete skupinu uživatelů, aplikace Kaspersky Endpoint Security výjimku nebude uplatňovat.

8. V poli **popis** zadejte popis výjimky.

9. Definujte nastavení zdrojového objektu nebo zdrojových procesů spuštěných objektem:

   - **Zdrojový proces**. Cesta nebo maska cesty k souboru nebo složce obsahující soubory (například `C:\Dir\File.exe` nebo `Dir\*.exe`).
   - **Hash zdrojového procesu**. Hodnota hash souboru.
   - **Zdrojový objekt**. Cesta nebo maska cesty k souboru nebo složce obsahující soubory (například `C:\Dir\File.exe` nebo `Dir\*.exe`). Například cesta k souboru `document.docm`, který používá skript nebo makro ke spuštění cílových procesů.

     Můžete také určit jiné objekty, které chcete vyloučit, jako je webová adresa, makro, příkaz v příkazovém řádku, cesta k registru nebo jiné. Určete objekt podle následující šablony: `object://<objekt>`, kde `<objekt>` odkazuje na název objektu, například `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Můžete také použít masky, například `object://*C:\Windows\temp\*`.
   - **Hash zdrojového objektu**. Hodnota hash souboru.

   Pravidlo součásti Adaptivní kontrola anomálií není použito na akce provedené objektem ani na procesy spuštěné objektem.

10. Určete nastavení cílového objektu nebo cílových procesů spuštěných v objektu.

    - **Cílový proces**. Cesta nebo maska cesty k souboru nebo složce obsahující soubory (například `C:\Dir\File.exe` nebo `Dir\*.exe`).
    - **Hash cílového procesu**. Hodnota hash souboru.
    - **Cílový objekt**. Příkaz ke spuštění cílového procesu. Zadejte příkaz pomocí následujícího vzoru: `object://<příkaz>`, například `object://cmdline:powershell -Command "$result = 'C:\windows\temp\result_local_users_pwdage txt'"`. Můžete také použít masky, například `object://*C:\windows\temp\*`.
    - **Hash cílového objektu**. Hodnota hash souboru.

    Pravidlo součásti Adaptivní kontrola anomálií není použito na akce provedené v objektu ani na procesy spuštěné v objektu.

11. Uložte změny.

Export and import výjimek pro pravidla součásti Adaptivní kontrola anomálií

Postup exportu nebo importu seznamu výjimek pro vybraná pravidla:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.

3. V bloku **Pravidla** klikněte na tlačítko **Upravit pravidla**.

   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií.

4. Postup exportu seznamu pravidel:

   a. Vyberte pravidlo, u nichž chcete exportovat výjimky.

   b. Klikněte na tlačítko **Exportovat**.

   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.

   d. Potvrďte, jestli chcete exportovat pouze vybrané výjimky, nebo exportovat celý seznam výjimek.

   e. Klikněte na tlačítko **Uložit**.

5. Postup importu seznamu pravidel:

   a. Klikněte na tlačítko **Importovat**.

   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.

   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.

6. Uložte změny.

Použití aktualizací pravidel součásti Adaptivní kontrola anomálií

Do tabulky pravidel lze přidat nová pravidla součásti Adaptivní kontrola anomálií a z tabulky pravidel lze odstranit existující pravidla součásti Adaptivní kontrola anomálií v případě aktualizace antivirových databází. Aplikace Kaspersky Endpoint Security odlišuje pravidla součásti Adaptivní kontrola anomálií, která mají být odstraněna nebo přidána do tabulky, pokud nebyla použita aktualizace těchto pravidel.

Dokud není aktualizace použita, zobrazuje aplikace Kaspersky Endpoint Security pravidla součásti Adaptivní kontrola anomálií, která budou aktualizací odstraněna, v tabulce pravidel a přiřadí jim stav *Zakázáno*. Nastavení těchto pravidel není možné měnit.

Postup použití aktualizací pravidel součásti Adaptivní kontrola anomálií:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.

3. V bloku **Pravidla** klikněte na tlačítko **Upravit pravidla**.

   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií.

4. V okně, které se otevře, klikněte na tlačítko **Schválit aktualizace**.

   Tlačítko **Schválit aktualizace** je dostupné v případě, že je k dispozici aktualizace pravidel součásti Adaptivní kontrola anomálií.

5. Uložte změny.

Úprava šablon zpráv součásti Adaptivní kontrola anomálií

Když se uživatel pokusí provést akci, která je zablokována pravidly součásti Adaptivní kontrola anomálií, aplikace Kaspersky Endpoint Security zobrazí zprávu, že jsou zablokovány potenciálně škodlivé akce. Pokud se uživatel domnívá, že akce byla omylem zablokována, může pomocí odkazu ve zprávě odeslat zprávu místnímu podnikovému správci sítě.

Jsou k dispozici speciální šablony pro zprávu o blokování potenciálně škodlivých akcí a pro zprávu, která bude odeslána správci. Tyto šablony zpráv můžete upravit.

Postup úpravy šablony zprávy:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnosti **Ochrana → Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.

3. V bloku **Šablony** nakonfigurujte šablony pro zprávy součásti Adaptivní kontrola anomálií:

   - **Blokování**. Šablona zprávy, která se zobrazí uživateli, když je spuštěno pravidlo součásti Adaptivní kontrola anomálií, které blokuje netypickou akci.

   - **Zpráva správci**. Šablona zprávy, kterou uživatel může zaslat správci místní podnikové sítě, pokud považuje blokování za chybu.

4. Uložte změny.

Zobrazení zpráv součásti Adaptivní kontrola anomálií

Postup zobrazení zpráv součásti Adaptivní kontrola anomálií:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V části **Kontrolní prvky zabezpečení** vyberte podčást **Adaptivní kontrola anomálií**.

   V pravé části okna se zobrazí nastavení součásti Adaptivní kontrola anomálií.

6. Proveďte jednu z následujících akcí:

- Chcete-li zobrazit zprávu o nastaveních pravidel součásti Adaptivní kontrola anomálií, klikněte na tlačítko **Zpráva o stavu pravidel**.
- Chcete-li zkontrolovat zprávu o spuštění pravidel součásti Adaptivní kontrola anomálií, klikněte na tlačítko **Zpráva o aktivaci pravidel**.

7. Spustí se proces generování zprávy.

Zpráva se zobrazí v novém okně.

Kontrola aplikací

Součást Kontrola aplikací řídí spouštění aplikací v počítačích uživatelů. Tím vám umožňuje implementovat podnikové zásady zabezpečení při používání aplikací. Součást Kontrola aplikací také snižuje riziko počítačové infekce omezením přístupu k aplikacím.

Konfigurace součásti Kontrola aplikací se skládá z následujících kroků:

1. Vytvoření kategorií aplikací.

   Správce vytvoří kategorie aplikací, které chce spravovat. Kategorie aplikací jsou určeny pro všechny počítače v podnikové síti bez ohledu na skupiny pro správu. Chcete-li vytvořit kategorii, můžete použít následující kritéria: Kategorie KL (například *Prohlížeče*), hodnota hash souboru, dodavatel aplikace a další kritéria.

2. Vytvoření pravidel součásti Kontrola aplikací.

   Správce vytvoří pravidla součástí Kontrola aplikací v zásadách pro skupinu správy. Pravidlo zahrnuje kategorie aplikace a stav spouštění aplikací z těchto kategorií: blokované nebo povolené.

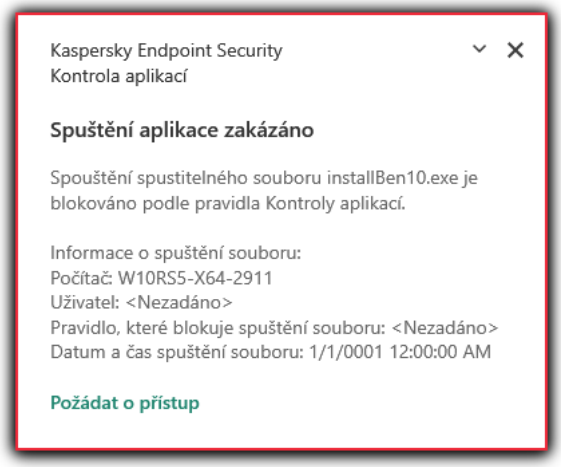
3. Volba režimu součásti Kontrola aplikací.

   Správce vybere režim pro práci s aplikacemi, které nejsou zahrnuty v žádném z pravidel (seznam blokovaných aplikací nebo seznam povolených aplikací).

Pokud se uživatel pokusí spustit zakázanou aplikaci, aplikace Kaspersky Endpoint Security její spuštění zablokuje a zobrazí upozornění (viz obrázek níže).

K dispozici je *testovací režim* pro kontrolu konfigurace součásti Kontrola aplikací. V tomto režimu aplikace Kaspersky Endpoint Security provádí následující akce:

- Umožňuje spouštění aplikací, včetně těch zakázaných.
- Zobrazuje oznámení o spuštění zakázané aplikace a přidá informace do zprávy v počítači uživatele.
- Odesílá data o spuštění zakázaných aplikací do aplikace Kaspersky Security Center.



Upozornění součásti Kontrola aplikací

Režimy operace součásti Kontrola aplikací

Součást Kontrola aplikací funguje ve dvou režimech:

- **Seznam blokovaných položek**. V tomto režimu umožňuje Kontrola aplikací uživatelům spouštět všechny aplikace kromě aplikací, které jsou v jejích pravidlech zakázány.

  Tento režim je ve výchozím nastavení povolen.

- **Seznam povolených položek**. V tomto režimu neumožňuje Kontrola aplikací uživatelům spouštět všechny aplikace kromě aplikací, které jsou v jejích pravidlech povoleny a nejsou zakázány.

  Pokud jsou pravidla povolených aplikací součástí Kontrola aplikací plně nakonfigurována, tato součást blokuje spouštění všech nových aplikací, které nebyly ověřeny správcem LAN, a zároveň umožňuje fungování operačního systému a důvěryhodných aplikací, které uživatelé potřebují pro práci.

  Můžete si přečíst doporučení ohledně konfigurace pravidel součásti Kontrola aplikací v režimu povolených aplikací.

Součást Kontrola aplikací lze nakonfigurovat tak, aby v těchto režimech fungovala jak pomocí místního rozhraní aplikace Kaspersky Endpoint Security, tak pomocí aplikace Kaspersky Security Center.

Aplikace Kaspersky Security Center však nabízí nástroje, které nejsou dostupné v místním rozhraní aplikace Kaspersky Endpoint Security, jako jsou například nástroje potřebné pro následující úkoly:

- Vytvoření kategorií aplikací.

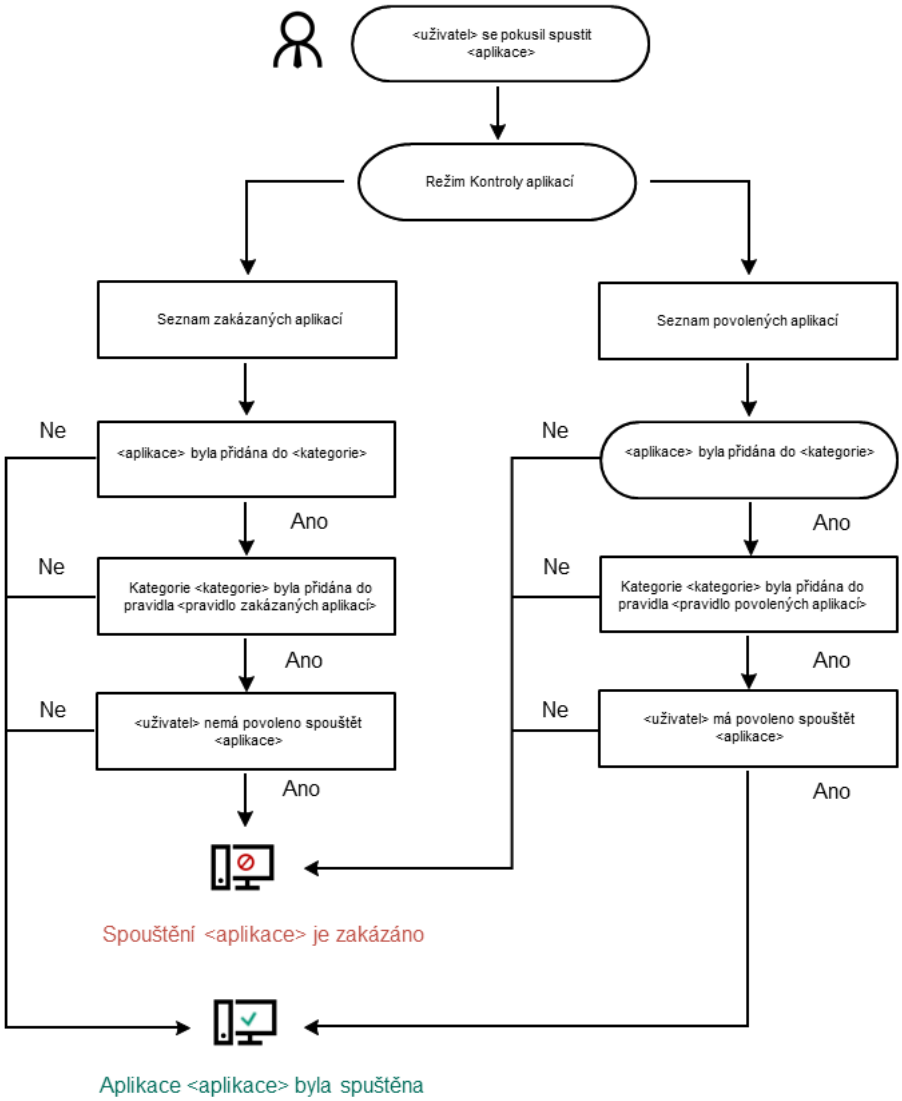
  Pravidla součásti Kontrola aplikací vytvořená v konzole pro správu aplikace Kaspersky Security Center jsou založena na vašich vlastních kategoriích aplikací, nikoli na podmínkách zahrnutí a vyloučení, jako je tomu v místním rozhraní aplikace Kaspersky Endpoint Security.

- Získávání informací o aplikacích nainstalovaných v počítačích v podnikové síti LAN.

Z tohoto důvodu se doporučuje používat aplikaci Kaspersky Security Center ke konfiguraci provozu součásti Kontrola aplikací.

Algoritmus činnosti součásti Kontrola aplikací

Aplikace Kaspersky Endpoint Security používá k rozhodnutí o spuštění aplikace algoritmus (viz obrázek níže).



Algoritmus činnosti součásti Kontrola aplikací

Omezení funkcí součásti Kontrola aplikací

Provoz součásti Kontrola aplikací je omezen v následujících případech:

- Při upgradu verze aplikace není podporován import nastavení součásti Kontrola aplikací.
- Když je upgradována verze aplikace, import nastavení součásti Kontrola aplikací je podporován pouze v případě, že je aplikace Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows nebo starší verze upgradována na aplikaci Kaspersky Endpoint Security 11.6.0 pro systém Windows.

  Když jsou upgradovány jiné verze aplikace než Kaspersky Endpoint Security 10 Service Pack 2 pro systém Windows, je nutné znovu nakonfigurovat nastavení součásti Kontrola aplikací, aby byl obnoven provozní stav této součásti.

- Pokud neexistuje spojení se servery služby KSN, aplikace Kaspersky Endpoint Security získává informace o reputaci aplikací a jejich modulech pouze z místních databází.

  Seznam aplikací přiřazených aplikací Kaspersky Endpoint Security ke kategorii KL **Applications trusted according to reputation in KSN** v případě dostupnosti připojení k serverů služby KSN se může lišit od seznamu aplikací přiřazených aplikací Kaspersky Endpoint Security ke kategorii KL **Applications trusted according to reputation in KSN** v případě nedostupnosti připojení ke službě KSN.

- V databázi aplikace Kaspersky Security Center je možné uložit informace o 150 000 zpracovaných souborech. Jakmile je dosaženo tohoto počtu záznamů, nebudou nové soubory zpracovány. Chcete-li obnovit inventarizaci, je nutné odstranit soubory, které byly předtím inventarizovány v databázi aplikace Kaspersky Security Center, z počítače s nainstalovanou aplikací Kaspersky Endpoint Security.

- Součást neřídí spouštění skriptů, pokud nejsou do překladače odesílány prostřednictvím příkazového řádku.

  Pokud je spuštění překladače povoleno pravidly součásti Kontrola aplikací, součást nebude blokovat skript spuštěný z tohoto překladače.

  Pokud pravidla součásti Kontrola aplikací blokují spuštění alespoň jednoho ze skriptů uvedených v příkazovém řádku překladače, součást blokuje všechny skripty uvedené v příkazovém řádku překladače.

- Součást neřídí spouštění skriptů z překladačů, které nejsou podporovány aplikací Kaspersky Endpoint Security.

  Aplikace Kaspersky Endpoint Security podporuje následující překladače:

  - Java.
  - PowerShell.

  Podporovány jsou následující typy překladačů:

  - %ComSpec%,
  - %SystemRoot%\\system32\\regedit.exe,
  - %SystemRoot%\\regedit.exe,
  - %SystemRoot%\\system32\\regedt32.exe,
  - %SystemRoot%\\system32\\cscript.exe,
  - %SystemRoot%\\system32\\wscript.exe,
  - %SystemRoot%\\system32\\msiexec.exe,
  - %SystemRoot%\\system32\\mshta.exe,
  - %SystemRoot%\\system32\\rundll32.exe,
  - %SystemRoot%\\system32\\wwahost.exe,
  - %SystemRoot%\\syswow64\\cmd.exe,

- %SystemRoot%\\syswow64\\regedit.exe,
- %SystemRoot%\\syswow64\\regedt32.exe,
- %SystemRoot%\\syswow64\\cscript.exe,
- %SystemRoot%\\syswow64\\wscript.exe,
- %SystemRoot%\\syswow64\\msiexec.exe,
- %SystemRoot%\\syswow64\\mshta.exe,
- %SystemRoot%\\syswow64\\rundll32.exe,
- %SystemRoot%\\syswow64\\wwahost.exe.

Povolení a zakázání součásti Kontrola aplikací

Součást Kontrola aplikací je ve výchozím nastavení zakázána.

Postup povolení nebo zakázání součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Pomocí přepínače **Kontrola aplikací** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je součást Kontrola aplikací povolena, aplikace bude předávat informace o spuštěných spustitelných souborech do aplikace Kaspersky Security Center. Seznam spuštěných spustitelných souborů můžete zobrazit v aplikaci Kaspersky Security Center ve složce **Spustitelné soubory**. Chcete-li dostávat informace o všech spustitelných souborech, nejen těch spuštěných, spusťte úlohu *Inventarizace*.

Volba režimu součásti Kontrola aplikací

Postup volby režimu součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. V bloku **Režim kontroly spouštění aplikací** vyberte některou z následujících možností:
   - **Seznam blokovaných položek**. Pokud je vybrána tato možnost, umožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel blokování součásti Kontrola aplikací.
   - **Seznam povolených položek**. Pokud je vybrána tato možnost, znemožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel povolení součásti Kontrola aplikací.

Původně definovanými pravidly pro režim Seznam povolených položek je pravidlo **Golden Image** a pravidlo **Důvěryhodné nástroje aktualizace**. Tato pravidla součásti Kontrola aplikací odpovídají kategoriím KL. Kategorie KL „Golden Image“ obsahuje programy, které zajišťují normální činnost operačního systému. Kategorie KL „Důvěryhodné nástroje aktualizace“ obsahuje nástroje aktualizace nejrenomovanějších dodavatelů softwaru. Tato pravidla nelze odstranit. Nastavení těchto pravidel nelze upravit. Ve výchozím nastavení je pravidlo **Golden Image** povoleno a pravidlo **Důvěryhodné nástroje aktualizace** zakázáno. Všichni uživatelé mohou spouštět aplikace, které odpovídají podmínkám aktivace pro tato pravidla.

Všechna pravidla vytvořená při použití vybraného režimu se uloží po změně režimu, aby bylo možné tato pravidla znovu použít. Chcete-li se vrátit k používání těchto pravidel, stačí vybrat požadovaný režim.

4. V části **Akce při spuštění blokovaných aplikací** vyberte akci, kterou má součást provést, když se uživatel pokusí spustit aplikaci blokovanou pravidly součásti Kontrola aplikací.

5. Pokud chcete, aby aplikace Kaspersky Endpoint Security monitorovala načítání modulů DLL při spouštění aplikací uživateli, zaškrtněte políčko **Řízení zavádění modulů DLL**.

   Informace o modulu a aplikaci, která modul načetla, se uloží do zprávy.

   Aplikace Kaspersky Endpoint Security monitoruje pouze moduly DLL a ovladače načtené od okamžiku zaškrtnutí políčka. Pokud chcete, aby aplikace Kaspersky Endpoint Security monitorovala všechny moduly DLL a ovladače, včetně těch, které byly načteny před spuštěním této aplikace, po zaškrtnutí políčka restartujte počítač.

   Při povolování kontroly načítání modulů DLL a ovladačů se ujistěte, že je v nastavení oddílu Kontrola aplikací povoleno jedno z následujících pravidel: výchozí pravidlo **Golden Image** nebo jiné pravidlo, které obsahuje kategorii KL „Důvěryhodné certifikáty“ a zajišťuje načtení důvěryhodných modulů DLL a ovladačů před spuštěním aplikace Kaspersky Endpoint Security. Povolení řízení načítání modulů DLL a ovladačů v případě zakázání pravidla **Golden Image** může způsobit nestabilitu v operačním systému.

   Doporučujeme zapnout ochranu heslem v případě konfigurace nastavení aplikace, aby bylo možné vypnout pravidla, která blokují spuštění kritických modulů DLL a ovladačů, bez nutnosti upravit nastavení zásad aplikace Kaspersky Security Center.

6. Uložte změny.

Práce s pravidly součásti Kontrola aplikací v rozhraní aplikace

Aplikace Kaspersky Endpoint Security kontroluje za použití pravidel spouštění aplikací uživateli. Pravidlo součásti Kontrola aplikací určuje podmínky aktivace a akce prováděné součástí Kontrola aplikací při aktivaci pravidla (povolení nebo blokování aplikací spouštěných uživateli).

Podmínky aktivace pravidla

Podmínka spouštění pravidel má následující korelaci: „typ podmínky – kritérium podmínky – hodnota podmínky“. Aplikace Kaspersky Endpoint Security použije (nebo nepoužije) na základě podmínek aktivace pravidla pravidlo na určitou aplikaci.

V pravidlech se používají následující typy podmínek:

- *Podmínky zahrnutí.* Aplikace Kaspersky Endpoint Security použije pravidlo na aplikaci, pokud tato aplikace odpovídá alespoň jedné podmínce zahrnutí.

- *Podmínky vyloučení.* Aplikace Kaspersky Endpoint Security nepoužije pravidlo na aplikaci, pokud tato aplikace odpovídá alespoň jedné podmínce vyloučení a nesplňuje žádnou z podmínek zahrnutí.

Podmínky aktivace pravidla jsou vytvářeny pomocí kritérií. K vytváření pravidel v aplikaci Kaspersky Endpoint Security se používají následující kritéria:

- Cesta ke složce, která obsahuje spustitelný soubor aplikace, nebo cesta ke spustitelnému souboru aplikace.

- Metadata: název spustitelného souboru aplikace, verze spustitelného souboru aplikace, název aplikace, verze aplikace, prodejce aplikace.

- Hodnota hash spustitelného souboru aplikace.

- Certifikát: vystavitel, předmět, kryptografický otisk.

- Zahrnutí aplikace do kategorie KL.

- Umístění spustitelného souboru aplikace na vyměnitelné jednotce.

Hodnota kritéria musí být zadána pro každé kritérium použité v podmínce. Pokud parametry spouštěné aplikace odpovídají hodnotám kritérií zadaným v podmínce zahrnutí, pravidlo se aktivuje. V tomto případě provede součást Kontrola aplikací akci popsanou v pravidle. Pokud parametry aplikace odpovídají hodnotám kritérií zadaným v podmínce vyloučení, součást Kontrola aplikací spouštění aplikace nekontroluje.

Akce provedené součástí Kontrola aplikací při aktivaci pravidla

Když je aktivováno nějaké pravidlo, součást Kontrola aplikací povolí uživatelům (nebo skupinám uživatelů) spouštět aplikace nebo zablokuje spuštění v souladu s pravidlem. Můžete vybrat jednotlivé uživatele nebo skupiny uživatelů, kteří mohou nebo nemohou spouštět aplikace aktivující určité pravidlo.

Pokud pravidlo neuvádí dané uživatele, kteří mohou spustit aplikace splňující podmínky daného pravidla, toto pravidlo se nazývá pravidlo *blokování*.

Pokud pravidlo neuvádí žádné uživatele, kteří nemohou spustit aplikace odpovídající danému pravidlu, toto pravidlo se nazývá pravidlo *povolení*.

Priorita pravidla blokování je vyšší než priorita pravidla povolení. Pokud bylo například pravidlo povolení v součásti Kontrola aplikací přiřazeno pro skupinu uživatelů a pravidlo blokování pro jednoho uživatele v této skupině uživatelů, tento uživatel nebude moci danou aplikaci spustit.

Provozní stav pravidla

Pravidla součásti Kontrola aplikací mohou mít některý z následujících provozních stavů:

- **Zap**. Tento stav značí, že pravidlo bude použito, pokud je aktivní součást Kontrola aplikací.

- **Vyp**. Tento stav značí, že pravidlo bude ignorováno, pokud je aktivní součást Kontrola aplikací.

- **Test**. Tento stav značí, že aplikace Kaspersky Endpoint Security povoluje spuštění aplikací, na která jsou pravidla použita, ale protokoluje informace o spuštění těchto aplikací do zprávy.

Přidání pravidla součásti Kontrola aplikací

Přidání nebo úprava pravidla součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Klikněte na tlačítko **Blokované aplikace** nebo **Povolené aplikace**.

   Tím otevřete seznam pravidel součásti Kontrola aplikací.
4. Klikněte na tlačítko **Přidat**.

   Otevře se okno **Pravidlo kontroly aplikací**.
5. Na kartě **Obecná nastavení** definujte hlavní nastavení pravidla:

   a. V poli **Název pravidla** zadejte název pravidla.

   b. V poli **Popis** zadejte popis pravidla.

   c. Zkompilujte nebo upravte seznam uživatelů a/nebo skupin uživatelů, kteří mají nebo nemají dovoleno spouštět aplikace splňující podmínky aktivace pravidla. To provedete tak, že v tabulce **Subjekty a jejich práva** kliknete na tlačítko **Přidat**.

   Ve výchozím nastavení je na seznam uživatelů přidána hodnota **Všichni**. Pravidlo platí pro všechny uživatele.

   > Pokud v tabulce není zadán žádný uživatel, pravidlo nelze uložit.

   d. V tabulce **Subjekty a jejich práva** pomocí přepínače definujte právo uživatelů spouštět aplikace.

   e. Zaškrtněte políčko **Zamítnout pro ostatní uživatele**, pokud chcete, aby všem uživatelům, kteří nejsou ve sloupci **Předmět** a nejsou součástí skupiny uživatelů zadané ve sloupci **Předmět**, bylo zakázáno spouštět aplikace odpovídající podmínkám aktivace pravidla.

   > Pokud není políčko **Zamítnout pro ostatní uživatele** zaškrtnuté, aplikace Kaspersky Endpoint Security nekontroluje spouštění aplikací uživateli, kteří nejsou zadáni v tabulce **Subjekty a jejich práva** a nepatří do skupiny uživatelů zadaných v tabulce **Subjekty a jejich práva**.

   f. Pokud chcete, aby aplikace Kaspersky Endpoint Security vyhodnotila aplikace odpovídající podmínkám aktivace pravidla jako důvěryhodné aktualizační nástroje s oprávněním vytvořit jiné spustitelné soubory, kterým bude povoleno následné spuštění, zaškrtněte políčko **Důvěryhodné nástroje aktualizace**.
6. Na kartě **Podmínky** vytvořte nebo upravte seznam podmínek zahrnutí pro spuštění pravidla.
7. Na kartě **Výjimky** vytvořte nebo upravte seznam podmínek výjimek pro spuštění pravidla.

   Při přenesení nastavení aplikace Kaspersky Endpoint Security je přenesen také seznam spustitelných souborů vytvořených důvěryhodnými nástroji aktualizace.
8. Uložte změny.

Přidání podmínky aktivace pro pravidlo součásti Kontrola aplikací

Postup přidání nové podmínky aktivace pro pravidlo součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Klikněte na tlačítko **Blokované aplikace** nebo **Povolené aplikace**.

   Tím otevřete seznam pravidel součásti Kontrola aplikací.
4. Vyberte pravidlo, pro které chcete nakonfigurovat podmínku spuštění.

   Otevře se okno pravidla součásti Kontrola aplikací.
5. Vyberte kartu **Podmínky** nebo kartu **Výjimky** a klikněte na tlačítko **Přidat**.
6. Vyberte podmínky aktivace pro pravidlo součásti Kontrola aplikací:

   - **Podmínky z vlastností spuštěných aplikací**. V seznamu spuštěných aplikací můžete vybrat aplikace, na které se použije pravidlo součásti Kontrola aplikací. Aplikace Kaspersky Endpoint Security také uvádí seznam aplikací, které byly dříve spuštěny v počítači. Musíte vybrat kritérium, které chcete použít k vytvoření jedné nebo více podmínek spuštění pravidla: **hodnota hash souboru**, **certifikát**, **kategorie KL**, **metadata** nebo **cesta ke složce**.
   - **Podmínky „kategorie KL“**. Položka *Kategorie KL* je seznam aplikací, které sdílely atributy motivu. Seznam je spravován odborníky společnosti Kaspersky. Například kategorie KL pro „Kancelářské aplikace“ zahrnuje aplikace ze sady Microsoft Office, aplikaci Adobe® Acrobat® a další.
   - **Vlastní podmínka**. Můžete vybrat soubor aplikace a vybrat jednu z podmínek spuštění pravidla: **hodnota hash souboru**, **certifikát**, **metadata** nebo **cesta k souboru nebo složce**.
   - **Stav podle disku souboru (vyměnitelný disk)**. Pravidlo součásti Kontrola aplikací se použije pouze na soubory spuštěné na vyměnitelné jednotce.
   - **Podmínky z vlastností souborů v zadané složce**. Pravidlo součásti Kontrola aplikací se použije pouze na soubory, které se nacházejí v zadané složce. Můžete také zahrnout nebo vyloučit soubory z podsložek. Musíte vybrat kritérium, které chcete použít k vytvoření jedné nebo více podmínek spuštění pravidla: **hodnota hash souboru**, **certifikát**, **kategorie KL**, **metadata** nebo **cesta ke složce**.
7. Uložte změny.

Při přidávání podmínek vezměte v úvahu následující zvláštní aspekty součásti Kontrola aplikací:

- Aplikace Kaspersky Endpoint Security nepodporuje hodnotu hash souboru MD5 a nekontroluje spouštění aplikací na základě algoritmu hash MD5. Jako podmínka aktivace pravidla se používá algoritmus hash SHA256.
- Jako podmínky aktivace pravidla nedoporučujeme používat jen kritéria **Vystavitel** a **Předmět**. Použití těchto kritérií je nespolehlivé.
- Pokud používáte symbolický odkaz v poli **Cesta k souboru nebo složce**, doporučujeme vám symbolický odkaz přeložit, aby pravidlo součásti Kontrola aplikací pracovalo správně. To provedete tak, že kliknete na tlačítko **Přeložit symbolický odkaz**.

Změna stavu pravidla součásti Kontrola aplikací

Postup změny stavu pravidla součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Klikněte na tlačítko **Blokované aplikace** nebo **Povolené aplikace**.
   Tím otevřete seznam pravidel součásti Kontrola aplikací.
4. Ve sloupci **Stav** otevřete kontextovou nabídku a vyberte některou z následujících možností:
   - **Zap**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo použito.
   - **Vyp**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo ignorováno.
   - **Testování**. Tento stav znamená, že aplikace Kaspersky Endpoint Security vždy povolí spuštění aplikací, na které je toto pravidlo použito, ale zaznamená informace o spuštění těchto aplikací do zprávy.
5. Uložte změny.

Správa pravidel součásti Kontrola aplikací v aplikaci Kaspersky Security Center

Aplikace Kaspersky Endpoint Security kontroluje za použití pravidel spouštění aplikací uživateli. Pravidlo součásti Kontrola aplikací určuje podmínky aktivace a akce prováděné součástí Kontrola aplikací při aktivaci pravidla (povolení nebo blokování aplikací spouštěných uživateli).

Podmínky aktivace pravidla

Podmínka spouštění pravidel má následující korelaci: „typ podmínky – kritérium podmínky – hodnota podmínky“. Aplikace Kaspersky Endpoint Security použije (nebo nepoužije) na základě podmínek aktivace pravidla pravidlo na určitou aplikaci.

V pravidlech se používají následující typy podmínek:

- *Podmínky zahrnutí.* Aplikace Kaspersky Endpoint Security použije pravidlo na aplikaci, pokud tato aplikace odpovídá alespoň jedné podmínce zahrnutí.
- *Podmínky vyloučení.* Aplikace Kaspersky Endpoint Security nepoužije pravidlo na aplikaci, pokud tato aplikace odpovídá alespoň jedné podmínce vyloučení a nesplňuje žádnou z podmínek zahrnutí.

Podmínky aktivace pravidla jsou vytvářeny pomocí kritérií. K vytváření pravidel v aplikaci Kaspersky Endpoint Security se používají následující kritéria:

- Cesta ke složce, která obsahuje spustitelný soubor aplikace, nebo cesta ke spustitelnému souboru aplikace.

- Metadata: název spustitelného souboru aplikace, verze spustitelného souboru aplikace, název aplikace, verze aplikace, prodejce aplikace.
- Hodnota hash spustitelného souboru aplikace.
- Certifikát: vystavitel, předmět, kryptografický otisk.
- Zahrnutí aplikace do kategorie KL.
- Umístění spustitelného souboru aplikace na vyměnitelné jednotce.

Hodnota kritéria musí být zadána pro každé kritérium použité v podmínce. Pokud parametry spouštěné aplikace odpovídají hodnotám kritérií zadaným v podmínce zahrnutí, pravidlo se aktivuje. V tomto případě provede součást Kontrola aplikací akci popsanou v pravidle. Pokud parametry aplikace odpovídají hodnotám kritérií zadaným v podmínce vyloučení, součást Kontrola aplikací spouštění aplikace nekontroluje.

Akce provedené součástí Kontrola aplikací při aktivaci pravidla

Když je aktivováno nějaké pravidlo, součást Kontrola aplikací povolí uživatelům (nebo skupinám uživatelů) spouštět aplikace nebo zablokuje spuštění v souladu s pravidlem. Můžete vybrat jednotlivé uživatele nebo skupiny uživatelů, kteří mohou nebo nemohou spouštět aplikace aktivující určité pravidlo.

Pokud pravidlo neuvádí dané uživatele, kteří mohou spustit aplikace splňující podmínky daného pravidla, toto pravidlo se nazývá pravidlo *blokování*.

Pokud pravidlo neuvádí žádné uživatele, kteří nemohou spustit aplikace odpovídající danému pravidlu, toto pravidlo se nazývá pravidlo *povolení*.

Priorita pravidla blokování je vyšší než priorita pravidla povolení. Pokud bylo například pravidlo povolení v součásti Kontrola aplikací přiřazeno pro skupinu uživatelů a pravidlo blokování pro jednoho uživatele v této skupině uživatelů, tento uživatel nebude moci danou aplikaci spustit.

Provozní stav pravidla

Pravidla součásti Kontrola aplikací mohou mít některý z následujících provozních stavů:

- **Zap**. Tento stav značí, že pravidlo bude použito, pokud je aktivní součást Kontrola aplikací.
- **Vyp**. Tento stav značí, že pravidlo bude ignorováno, pokud je aktivní součást Kontrola aplikací.

Test. Tento stav značí, že aplikace Kaspersky Endpoint Security povoluje spuštění aplikací, na která jsou pravidla použita, ale protokoluje informace o spuštění těchto aplikací do zprávy.

Získávání informací o aplikacích nainstalovaných v počítačích uživatelů

Chcete-li vytvořit optimální pravidla součásti Kontrola aplikací, doporučujeme vám nejprve získat přehled o aplikacích, které jsou používány v počítačích ve firemní síti LAN. V tomto směru je vhodné zjistit následující informace:

- dodavatelé, verze a lokalizace aplikací používaných ve firemní síti LAN;
- frekvence aktualizace aplikací;

- zásady používání aplikací v rámci společnosti (může se jednat o bezpečnostní i administrativní zásady);
- umístění úložiště distribučních balíčků aplikací.

Informace o aplikacích, které jsou používány v počítačích firemní sítě LAN, jsou k dispozici ve složkách **Applications registry** a **Executable files**. Složky **Applications registry** a **Executable files** se nacházejí ve složce **Application management** ve stromu konzole pro správu aplikace Kaspersky Security Center.

Složka **Applications registry** obsahuje seznam aplikací zjištěných součástí Network Agent, která je instalována v klientských počítačích.

Složka **Executable files** obsahuje seznam všech spustitelných souborů, které kdy byly v klientských počítačích spuštěny nebo které byly zjištěny během úlohy inventarizace aplikace Kaspersky Endpoint Security.

Obecné informace o aplikaci a jejích spustitelných souborech a také seznam počítačů, ve kterých je aplikace instalována, najdete v okně vlastností aplikace, která je vybrána ve složce **Applications registry** nebo **Executable files**.

*Postup otevření okna vlastností u aplikací ve složce **Applications registry**:*

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly pro správu vyberte možnosti **Additional** → **Application management** → složku **Applications registry**.
3. Vyberte aplikaci.
4. V kontextové nabídce aplikace vyberte možnost **Properties**.

*Postup otevření okna vlastností u spustitelného souboru ve složce **Executable files**:*

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole pro správu vyberte možnosti **Additional** → **Application management** → složku **Executable files**.
3. Vyberte spustitelný soubor.
4. V kontextové nabídce spustitelného souboru vyberte možnost **Properties**.

Vytváření kategorií aplikací

Aby bylo vytváření pravidel součásti Kontrola aplikací snazší, můžete vytvářet kategorie aplikací.

Doporučujeme vám vytvořit kategorii „pracovních aplikací“, která zahrne standardní sadu aplikací používaných v rámci společnosti. Pokud různé skupiny uživatelů používají ke své práci různé sady aplikací, lze pro jednotlivé skupiny vytvořit samostatné kategorie aplikací.

Postup vytvoření kategorie aplikací:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole pro správu vyberte možnosti **Additional** → **Application management** → složku **Application categories**.

3. Klikněte na tlačítko **Create category** v pracovním prostoru.

   Spustí se průvodce vytvořením kategorie uživatelů.

4. Postupujte podle pokynů průvodce vytvořením kategorie uživatelů.

Krok 1. Volba typu kategorie

V tomto kroku vyberte jeden z následujících typů kategorií aplikací:

- **Kategorie s ručně přidaným obsahem**. Pokud jste vybrali tento typ kategorie, v kroku „Konfigurace podmínek zahrnutí aplikace do kategorie“ a v kroku „Konfigurace podmínek vyloučení aplikací z kategorie“ budete moci definovat kritéria, podle kterých budou spustitelné soubory zahrnuty do příslušné kategorie.
- **Kategorie zahrnující spustitelné soubory z vybraných zařízení**. Pokud jste vybrali tento typ kategorie, v kroku „Nastavení“ budete moci určit počítač, jehož spustitelné soubory budou automaticky zahrnuty do kategorie.
- **Kategorie zahrnující spustitelné soubory z konkrétní složky**. Pokud jste vybrali tento typ kategorie, v kroku „Složka úložiště“ budete moci určit složku, jejíž spustitelné soubory budou automaticky zahrnuty do příslušné kategorie.

Při vytváření kategorie s automaticky přidaným obsahem provede aplikace Kaspersky Security Center inventarizaci souborů s následujícími formáty: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX a SCR.

Krok 2. Zadání názvu kategorie uživatelů

V tomto kroku určete název kategorie aplikací.

Krok 3. Konfigurace podmínek zahrnutí aplikací do kategorie

Tento krok je dostupný v případě, že jste vybrali typ kategorie **Kategorie s ručně přidaným obsahem**.

V tomto kroku vyberte v rozevíracím seznamu **Přidat** podmínky zahrnutí aplikací do kategorie:

- **From the list of executable files**. Přidejte aplikace ze seznamu spustitelných souborů v klientském zařízení do vlastní kategorie.
- **From file properties**. Určete podrobná data spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.
- **Metadata from files in folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory. Aplikace Kaspersky Security Center určí metadata těchto spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.
- **Checksums of files in folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory. Aplikace Kaspersky Security Center určí hodnoty hash těchto spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.
- **Certificates for files from folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory podepsané certifikáty. Aplikace Kaspersky Security Center určí certifikáty těchto spustitelných souborů jako

podmínku přidání aplikací do vlastní kategorie.

Nedoporučuje se používat podmínky, jejichž vlastnosti nemají určený parametr **Kryptografický otisk certifikátu**.

- **MSI installer files metadata**. Vyberte balíček MSI. Aplikace Kaspersky Security Center určí metadata spustitelných souborů zabalených v tomto instalačním balíčku MSI jako podmínku přidání aplikací do vlastní kategorie.
- **Checksums of files from MSI installer of the application**. Vyberte balíček MSI. Aplikace Kaspersky Security Center určí hodnoty hash spustitelných souborů zabalených v tomto instalačním balíčku jako podmínku přidání aplikací do vlastní kategorie.
- **Kategorie KL**. Určete kategorii KL jako podmínku přidání aplikací do vlastní kategorie. Položka *Kategorie KL* je seznam aplikací, které sdílely atributy motivu. Seznam je spravován odborníky společnosti Kaspersky. Například kategorie KL známá jako „Kancelářské aplikace“ zahrnuje aplikace ze sady Microsoft Office, aplikaci Adobe Acrobat a další.

  Můžete vybrat všechny kategorie KL a vygenerovat rozšířený seznam důvěryhodných aplikací.
- **Path to application**. V klientském zařízení vyberte složku. Aplikace Kaspersky Security Center přidá spustitelné soubory z této složky do vlastní kategorie.
- **Certificates from certificate repository**. Vyberte certifikáty, které byly použity k podepsání spustitelných souborů, jako podmínku pro přidání aplikací do vlastní kategorie.

  Nedoporučuje se používat podmínky, jejichž vlastnosti nemají určený parametr **Kryptografický otisk certifikátu**.
- **Drive type**. Určete typ paměťového zařízení (všechny pevné disky a vyměnitelné jednotky nebo pouze vyměnitelné jednotky) jako podmínku přidání aplikací do vlastní kategorie.

Krok 4. Konfigurace podmínek vyloučení aplikací z kategorie

Tento krok je dostupný v případě, že jste vybrali typ kategorie **Kategorie s ručně přidaným obsahem**.

Aplikace určené v tomto kroku jsou vyloučeny z kategorie, i když byly tyto aplikace určeny v kroku „Konfigurace podmínek zahrnutí aplikací do kategorie“.

V tomto kroku vyberte v rozevíracím seznamu **Přidat** podmínky vyloučení aplikací z kategorie:

- **From the list of executable files**. Přidejte aplikace ze seznamu spustitelných souborů v klientském zařízení do vlastní kategorie.
- **From file properties**. Určete podrobná data spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.
- **Metadata from files in folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory. Aplikace Kaspersky Security Center určí metadata těchto spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.

- **Checksums of files in folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory. Aplikace Kaspersky Security Center určí hodnoty hash těchto spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.

- **Certificates for files from folder**. V klientském zařízení vyberte složku, která obsahuje spustitelné soubory podepsané certifikáty. Aplikace Kaspersky Security Center určí certifikáty těchto spustitelných souborů jako podmínku přidání aplikací do vlastní kategorie.

- **MSI installer files metadata**. Vyberte balíček MSI. Aplikace Kaspersky Security Center určí metadata spustitelných souborů zabalených v tomto instalačním balíčku MSI jako podmínku přidání aplikací do vlastní kategorie.

- **Checksums of files from MSI installer of the application**. Vyberte balíček MSI. Aplikace Kaspersky Security Center určí hodnoty hash spustitelných souborů zabalených v tomto instalačním balíčku jako podmínku přidání aplikací do vlastní kategorie.

- **Kategorie KL**. Určete kategorii KL jako podmínku přidání aplikací do vlastní kategorie. Položka *Kategorie KL* je seznam aplikací, které sdílely atributy motivu. Seznam je spravován odborníky společnosti Kaspersky. Například kategorie KL známá jako „Kancelářské aplikace“ zahrnuje aplikace ze sady Microsoft Office, aplikaci Adobe Acrobat a další.

  Můžete vybrat všechny kategorie KL a vygenerovat rozšířený seznam důvěryhodných aplikací.

- **Path to application**. V klientském zařízení vyberte složku. Aplikace Kaspersky Security Center přidá spustitelné soubory z této složky do vlastní kategorie.

- **Certificates from certificate repository**. Vyberte certifikáty, které byly použity k podepsání spustitelných souborů, jako podmínku pro přidání aplikací do vlastní kategorie.

- **Drive type**. Určete typ paměťového zařízení (všechny pevné disky a vyměnitelné jednotky nebo pouze vyměnitelné jednotky) jako podmínku přidání aplikací do vlastní kategorie.

Krok 5. Nastavení

Tento krok je k dispozici v případě, že jste vybrali typ kategorie **Kategorie zahrnující spustitelné soubory z vybraných zařízení**.

V tomto kroku klikněte na tlačítko **Přidat** a určete počítače, jejichž spustitelné soubory budou aplikací Kaspersky Security Center přidány do kategorie aplikací. Všechny spustitelné soubory z určených počítačů přítomné ve složce **Spustitelné soubory** budou aplikací Kaspersky Security Center přidány do kategorie aplikací.

V tomto kroku můžete také nakonfigurovat následující nastavení:

- Algoritmus výpočtu funkce hodnoty hash pomocí aplikace Kaspersky Security Center. Chcete-li vybrat algoritmus, je nutné zaškrtnout alespoň jedno z následujících políček:

  - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)**.

  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- Zaškrtávací políčko **Synchronize data with the Administration Server repository**. Toto políčko zaškrtněte, pokud chcete, aby aplikace Kaspersky Security Center pravidelně vymazala kategorii aplikací a přidala do ní všechny spustitelné soubory z určených počítačů přítomných ve složce **Spustitelné soubory**.

Pokud není zaškrtnuto políčko **Synchronize data with the Administration Server repository**, aplikace Kaspersky Security Center neprovede žádné úpravy kategorie aplikací po jejím vytvoření.

- Pole **Scan period (h)**. V tomto poli můžete určit dobu (v hodinách), po které aplikace Kaspersky Security Center vymaže kategorii aplikací a přidá do ní všechny spustitelné soubory z určených počítačů přítomných ve složce **Spustitelné soubory**.

  Pole je dostupné v případě, že je zaškrtnuto políčko **Synchronize data with the Administration Server repository**.

Krok 6. Složka úložiště

Tento krok je k dispozici v případě, že jste vybrali typ kategorie **Kategorie zahrnující spustitelné soubory z konkrétní složky**.

V tomto kroku klikněte na tlačítko **Procházet** a určete složku, ve které aplikace Kaspersky Security Center vyhledá spustitelné soubory a automaticky přidá aplikace do kategorie aplikací.

V tomto kroku můžete také nakonfigurovat následující nastavení:

- Zaškrtávací políčko **Include dynamic-link libraries (DLL) in this category**. Toto políčko zaškrtněte, pokud chcete, aby byly do kategorie aplikace zahrnuty knihovny dynamických odkazů (soubory DLL).

  Zahrnutí souborů DLL do kategorie aplikací může snížit výkon aplikace Kaspersky Security Center.

- Zaškrtávací políčko **Include script data in this category**. Toto políčko zaškrtněte, pokud chcete, aby byly do kategorie aplikace zařazeny skripty.

  Zahrnutí skriptů do kategorie aplikace může snížit výkon aplikace Kaspersky Security Center.

- Algoritmus výpočtu funkce hodnoty hash pomocí aplikace Kaspersky Security Center. Chcete-li vybrat algoritmus, je nutné zaškrtnout alespoň jedno z následujících políček:

  - **Calculate SHA-256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and any later versions)**.

  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- Zaškrtávací políčko **Force folder scan for changes**. Toto políčko zaškrtněte, pokud chcete, aby aplikace Kaspersky Security Center pravidelně vyhledala spustitelné soubory ve složce použité k automatickému přidání do kategorie aplikací.

  Pokud není políčko **Force folder scan for changes** zaškrtnuto, aplikace Kaspersky Security Center vyhledá spustitelné soubory ve složce použité k automatickému přidání do kategorie aplikací pouze v případě, že ve složce byly provedeny změny, byly do ní přidány soubory nebo z ní byly odstraněny.

- Pole **Scan period (h)**. V tomto poli můžete určit časový interval (v hodinách), po kterém aplikace Kaspersky Security Center vyhledá spustitelné soubory ve složce použité k automatickému přidání do kategorie aplikací.

  Toto pole je dostupné v případě, že je zaškrtnuto políčko **Force folder scan for changes**.

Krok 7. Vytvoření vlastní kategorie

Chcete-li průvodce instalací aplikace ukončit, klikněte na tlačítko **Dokončit**.

Přidání spustitelných souborů ze složky Executable files do kategorie aplikací

Ve složce **Executable files** je zobrazen seznam spustitelných souborů zjištěných v počítačích. Aplikace Kaspersky Endpoint Security po provedení úlohy inventarizace vygeneruje seznam spustitelných souborů.

*Postup přidání souborů ze složky **Executable files** do kategorie aplikací:*

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole pro správu vyberte možnosti **Additional** → **Application management** → složku **Executable files**.
3. V pracovním prostoru vyberte spustitelné soubory, které chcete přidat do kategorie aplikací.
4. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku vybraných spustitelných souborů a vyberte možnost **Add to category**.

   Otevře se okno **Select application category**.
5. V okně **Select application category**:
   - V horní části okna vyberte jednu z následujících možností:
     - **Create category of applications**. Tuto možnost vyberte, pokud chcete vytvořit novou kategorii aplikací a přidat do ní spustitelné soubory.
     - **Add rules to specified category**. Tuto možnost vyberte, pokud chcete vybrat stávající kategorii aplikací a přidat do ní spustitelné soubory.
   - V části **Rule type** vyberte jednu z následujících možností:
     - **Add to inclusion rules**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která do kategorii aplikací přidá spustitelné soubory.
     - **Add to exclusion rules**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která z kategorie aplikací vyloučí spustitelné soubory.
   - V části **File info type** vyberte jednu z následujících možností:
     - **Certificate data (or SHA-256 for files without a certificate)**.
     - **Certificate data (files without a certificate will be skipped)**.
     - **Only SHA-256 (files without SHA-256 will be skipped)**.
     - **MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1)**.
6. Klikněte na tlačítko **OK**.

Přidání spustitelných souborů souvisejících s událostmi do kategorie aplikací

Postup přidání spustitelných souborů souvisejících s událostmi součásti Kontrola aplikací do kategorie aplikací:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** ve stromu konzole pro správu vyberte kartu **Events**.
3. V rozevíracím seznamu **Selection events** zvolte výběr událostí týkajících se činnosti součásti Kontrola aplikací (Zobrazení událostí vyplývajících z provozu součásti Kontrola aplikací, Zobrazení událostí vyplývajících z testovacího provozu součásti Kontrola aplikací).
4. Klikněte na tlačítko **Run selection**.
5. Vyberte události, jejichž související spustitelné soubory chcete přidat do kategorie aplikací.
6. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku vybraných událostí a vyberte možnost **Add to category**.

   Otevře se okno **Select application category**.
7. V okně **Select application category**:
   - V horní části okna vyberte jednu z následujících možností:
     - **Create category of applications**. Tuto možnost vyberte, pokud chcete vytvořit novou kategorii aplikací a přidat do ní spustitelné soubory.
     - **Add rules to specified category**. Tuto možnost vyberte, pokud chcete vybrat stávající kategorii aplikací a přidat do ní spustitelné soubory.
   - V části **Rule type** vyberte jednu z následujících možností:
     - **Add to inclusion rules**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která do kategorii aplikací přidá spustitelné soubory.
     - **Add to exclusion rules**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která z kategorie aplikací vyloučí spustitelné soubory.
   - V části **File info type** vyberte jednu z následujících možností:
     - **Certificate data (or SHA-256 for files without a certificate)**.
     - **Certificate data (files without a certificate will be skipped)**.
     - **Only SHA-256 (files without SHA-256 will be skipped)**.
     - **MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1)**.
8. Klikněte na tlačítko **OK**.

Přidání a úprava pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center

Přidání nebo úprava pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Kontrolní prvky zabezpečení → Kontrola aplikací**.

   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.
6. Proveďte jednu z následujících akcí:

   - Po kliknutí na tlačítko **Přidat** můžete přidat pravidlo.
   - Pokud chcete upravit stávající pravidlo, vyberte je v seznamu pravidel a klikněte na tlačítko **Upravit**.

   Otevře se okno **Pravidlo kontroly aplikací**.
7. Proveďte jednu z následujících akcí:

   - Chcete-li vytvořit novou kategorii:

     a. Klikněte na tlačítko **Vytvořit kategorii**.

     Spustí se průvodce vytvořením kategorie uživatelů.

     b. Postupujte podle pokynů průvodce vytvořením kategorie uživatelů.

     c. V rozevíracím seznamu **Kategorie** vyberte vytvořenou kategorii aplikací.
   - Chcete-li upravit stávající kategorii:

     a. V rozevíracím seznamu **Kategorie** vyberte vytvořenou kategorii aplikací, kterou chcete upravit.

     b. Klikněte na tlačítko **Vlastnosti**.

     Otevře se okno **Vlastnosti: <Název kategorie>**.

     c. Upravte nastavení vybrané kategorie aplikací.

     d. Klikněte na tlačítko **OK**.

     e. V rozevíracím seznamu **Kategorie** vyberte vytvořenou kategorii aplikací, na základě které chcete vytvořit pravidlo.
8. V tabulce **Subjekty a jejich práva** kliknete na tlačítko **Přidat**.

   Otevře se standardní okno systému Microsoft Windows **Vybrat uživatele nebo skupiny**.

9. V okně **Vybrat uživatele nebo skupiny** určete seznam uživatelů či skupin uživatelů, pro které chcete nakonfigurovat oprávnění ke spouštění aplikací z vybrané kategorie.

10. V tabulce **Subjekty a jejich práva**:

    - Pokud chcete uživatelům či skupinám uživatelů povolit spouštění aplikací patřících do vybrané kategorie, zaškrtněte políčko **Povolit** na příslušných řádcích.

    - Pokud chcete uživatelům či skupinám uživatelů zakázat spouštění aplikací patřících do vybrané kategorie, zaškrtněte políčko **Zamítnout** na příslušných řádcích.

11. Zaškrtněte políčko **Zamítnout pro ostatní uživatele**, pokud chcete, aby všem uživatelům, kteří nejsou ve sloupci **Předmět** a nejsou součástí skupiny uživatelů zadané ve sloupci **Předmět**, bylo zakázáno spouštět aplikace patřící do vybrané kategorie.

12. Pokud chcete, aby aplikace Kaspersky Endpoint Security vyhodnotila aplikace obsažené ve vybrané kategorii aplikací jako důvěryhodné aktualizační nástroje s oprávněním vytvořit jiné spustitelné soubory, kterým bude následně povoleno spuštění, zaškrtněte políčko **Důvěryhodné nástroje aktualizace**.

    Při přenesení nastavení aplikace Kaspersky Endpoint Security je přenesen také seznam spustitelných souborů vytvořených důvěryhodnými nástroji aktualizace.

13. Uložte změny.

Změna stavu pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center

Postup změny stavu pravidla součásti Kontrola aplikací:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V okně zásad vyberte možnost **Kontrolní prvky zabezpečení → Kontrola aplikací**.

   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.

6. Ve sloupci **Stav** kliknutím levým tlačítkem zobrazte kontextovou nabídku a vyberte některou z následujících možností:

    - **Zap**. Tento stav značí, že pravidlo bude použito, pokud je aktivní součást Kontrola aplikací.

    - **Vyp**. Tento stav značí, že pravidlo bude ignorováno, pokud je aktivní součást Kontrola aplikací.

    - **Test**. Tento stav znamená, že aplikace Kaspersky Endpoint Security vždy povolí spuštění aplikací, pro které pravidlo platí, ale zaznamená informace o spuštění těchto aplikací do zprávy.

Pomocí stavu **Test** můžete přiřadit akci odpovídající možnosti **Otestovat pravidla** pro část pravidel, když je v rozevíracím seznamu **Akce** vybrána možnost **Použít pravidla**.

7. Uložte změny.

Export a import pravidel součásti Kontrola aplikací

Seznam pravidel součásti Kontrola aplikací můžete exportovat do souboru XML. Můžete použít funkci exportu/importu k zálohování seznamu pravidel součásti Kontrola aplikací nebo k migraci seznamu na jiný server.

Při exportu a importu pravidel Kontrola aplikací mějte na mysli následující zvláštní aspekty:

- Aplikace Kaspersky Endpoint Security exportuje seznam pravidel pouze pro aktivní režim součásti Kontrola aplikací. Jinými slovy, pokud Kontrola aplikací funguje v režimu zakázaných položek, aplikace Kaspersky Endpoint Security exportuje pravidla pouze pro tento režim. Chcete-li exportovat seznam pravidel pro režim povolených položek, musíte přepnout režim a spustit operaci exportu znovu.

- Aby mohla pravidla součásti Kontrola aplikací fungovat, aplikace Kaspersky Endpoint Security používá kategorie aplikací. Při migrování seznamu pravidel součásti Kontrola aplikací na jiný server musíte také migrovat seznam kategorií aplikací. Další informace o exportu nebo importu kategorií aplikací *najdete v nápovědě k aplikaci Kaspersky Security Center*.

Jak exportovat a importovat seznam pravidel součásti Kontrola aplikací v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
6. Postup exportu seznamu pravidel součásti Kontrola aplikací:
   a. Vyberte pravidla, která chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádné pravidlo nevybrali, aplikace Kaspersky Endpoint Security exportuje všechna pravidla.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
7. Postup exportu seznamu pravidel součásti Kontrola aplikací:
   a. Klikněte na odkaz **Importovat**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

[Jak exportovat a importovat seznam pravidel součásti Kontrola aplikací ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam pravidel.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
5. Klikněte na odkaz **Nastavení seznamů pravidel**.
6. Vyberte seznam pravidel: seznam zakázaných aplikací nebo seznam povolených.
7. Postup exportu seznamu pravidel součásti Kontrola aplikací:
   a. Vyberte pravidla, která chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrd'te, jestli chcete exportovat pouze vybraná pravidla, nebo exportovat celý seznam pravidel.
   d. Klikněte na tlačítko **Exportovat**.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML ve výchozí složce pro stahování.
8. Postup exportu seznamu pravidel součásti Kontrola aplikací:
   a. Klikněte na odkaz **Importovat**.

      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
9. Uložte změny.

Testování pravidel součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center

Aby pravidla součásti Kontrola aplikací neblokovala aplikace, jejichž provoz je vyžadovaný, doporučujeme povolit testování pravidel kontroly aplikací a analyzovat jejich funkci po vytvoření nových pravidel. Když je povoleno testování pravidel součásti Kontrola aplikací, aplikace Kaspersky Endpoint Security nebude blokovat aplikace, jejichž spouštění je zakázáno součástí Kontrola aplikací, ale místo toho odešle upozornění o jejich spuštění na administrační server.

Analýza funkce pravidel součásti Kontrola aplikací vyžaduje prohlédnutí výsledných událostí součásti Kontrola aplikací, které budou hlášeny do aplikace Kaspersky Security Center. Pokud má testovací režim za následek, že nejsou blokovány žádné události spuštění u všech aplikací potřebných pro práci uživatele počítače, znamená to, že byla vytvořena správná pravidla. V opačném případě vám doporučujeme aktualizovat nastavení pravidel, která jste vytvořili, vytvořit další pravidla nebo odstranit stávající pravidla.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security umožňuje spouštění všech aplikací s výjimkou aplikací, které pravidla zakazují.

Postup povolení nebo zakázání testování pravidel součásti Kontrola aplikací v Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Kontrolní prvky zabezpečení → Kontrola aplikací**.

   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.
6. V rozevíracím seznamu **Režim kontroly aplikací** vyberte jednu z následujících položek:

   - **Seznam blokovaných položek**. Pokud je vybrána tato možnost, umožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel blokování součásti Kontrola aplikací.
   - **Seznam povolených položek**. Pokud je vybrána tato možnost, znemožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel povolení součásti Kontrola aplikací.
7. Proveďte jednu z následujících akcí:

   - Chcete-li povolit testování pravidel součásti Kontrola aplikací, v rozevíracím seznamu **Akce** vyberte možnost **Otestovat pravidla**.
   - Pokud chcete povolit součást Kontrola aplikací, aby mohla spravovat spouštění aplikací v počítačích uživatelů, vyberte možnost **Použít pravidla** v rozevíracím seznamu **Akce**.
8. Uložte změny.

Zobrazení událostí vyplývajících z testovacího provozu součásti Kontrola aplikací

Postup zobrazení událostí součásti Kontrola aplikací přijatých aplikací Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** ve stromu konzole pro správu vyberte kartu **Events**.
3. Klikněte na tlačítko **Create a selection**.

Otevře se okno **Properties: <Název výběru>**.

4. Otevřete část **Události**.
5. Klikněte na tlačítko **Vymazat vše**.
6. Na kartě **Události** zaškrtněte políčka **Spuštění aplikace zakázáno v režimu testování** a **Spuštění aplikace povoleno v režimu testování**.
7. Klikněte na tlačítko **OK**.
8. V rozevíracím seznamu **Selection events** vyberte vytvořený výběr.
9. Klikněte na tlačítko **Run selection**.

Zobrazení zprávy o blokovaných aplikacích v testovacím režimu

Postup zobrazení zprávy o blokovaných aplikacích v testovacím režimu:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** stromu konzole pro správu vyberte kartu **Reports**.
3. Klikněte na tlačítko **New report template**.

   Spustí se průvodce Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V kroku **Selecting the report template type** vyberte možnost **Other** a poté **Report on blocked applications in test mode**.

   Jakmile budete s průvodcem New Report Template Wizard hotovi, zobrazí se nová šablona zprávy v tabulce na kartě **Reports**.
5. Dvojitým kliknutím na zprávu ji otevřete.

Spustí se proces generování zprávy. Zpráva se zobrazí v novém okně.

Zobrazení událostí vyplývajících z provozu součásti Kontrola aplikací

Postup zobrazení událostí vyplývajících z funkce součásti Kontrola aplikací, které byly přijaty aplikací Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** ve stromu konzole pro správu vyberte kartu **Events**.
3. Klikněte na tlačítko **Create a selection**.

   Otevře se okno **Properties: <Název výběru>**.
4. Otevřete část **Události**.
5. Klikněte na tlačítko **Vymazat vše**.

6. V tabulce **Události** zaškrtněte políčko **Spuštění aplikace zakázáno**.
7. Klikněte na tlačítko **OK**.
8. V rozevíracím seznamu **Selection events** vyberte vytvořený výběr.
9. Klikněte na tlačítko **Run selection**.

Zobrazení zprávy o blokovaných aplikacích

Postup zobrazení zprávy o blokovaných aplikacích:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** stromu konzole pro správu vyberte kartu **Reports**.
3. Klikněte na tlačítko **New report template**.

   Spustí se průvodce Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V kroku **Selecting the report template type** vyberte možnost **Other** a poté **Report on blocked applications**.

   Jakmile budete s průvodcem New Report Template Wizard hotovi, zobrazí se nová šablona zprávy v tabulce na kartě **Reports**.
5. Dvojitým kliknutím na zprávu ji otevřete.

Spustí se proces generování zprávy. Zpráva se zobrazí v novém okně.

Testování pravidel součásti Kontrola aplikací

Aby pravidla součásti Kontrola aplikací neblokovala aplikace, jejichž provoz je vyžadovaný, doporučujeme povolit testování pravidel kontroly aplikací a analyzovat jejich funkci po vytvoření nových pravidel.

Analýza funkce pravidel součásti Kontrola aplikací vyžaduje prohlédnutí výsledných událostí součásti Kontrola aplikací, které budou hlášeny do aplikace Kaspersky Security Center. Pokud má testovací režim za následek, že nejsou blokovány žádné události spuštění u všech aplikací potřebných pro práci uživatele počítače, znamená to, že byla vytvořena správná pravidla. V opačném případě vám doporučujeme aktualizovat nastavení pravidel, která jste vytvořili, vytvořit další pravidla nebo odstranit stávající pravidla.

Postup povolení testování pravidel součásti Kontrola aplikací nebo výběru akce blokování u součásti Kontrola aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.

   Tím otevřete seznam pravidel součásti Kontrola aplikací.
3. Ve sloupci **Stav** vyberte možnost **Testování**.

   Tento stav znamená, že aplikace Kaspersky Endpoint Security vždy povolí spuštění aplikací, na které je toto pravidlo použito, ale zaznamená informace o spuštění těchto aplikací do zprávy.

4. Uložte změny.

Aplikace Kaspersky Endpoint Security nebude blokovat aplikace, jejichž spouštění je zakázáno součástí Kontrola aplikací, ale odešle upozornění o jejich spuštění na administrační server.

Monitor aktivity aplikací

Monitor aktivity aplikací je nástroj navržený k zobrazování informací o aktivitě aplikací uživatelského počítače v reálném čase.

Používání Monitoru aktivity aplikací vyžaduje instalaci součástí Kontrola aplikací a Prevence narušení hostitele. Pokud tyto součásti nejsou nainstalovány, část Monitor aktivity aplikací v hlavním okně aplikace je skrytá.

Postup spuštění součásti Monitor aktivity aplikací:

V hlavním okně aplikace klikněte na **Další nástroje** → **Monitor aktivity aplikací**.

Otevře se okno **Aktivita aplikací**. V tomto okně se na třech kartách zobrazují informace o aktivitě aplikací na počítači uživatele:

- Na kartě **Všechny aplikace** se zobrazují informace o všech aplikacích nainstalovaných na počítači.
- Na kartě **Spuštěno** se zobrazují informace o využití prostředků počítače jednotlivými aplikacemi v reálném čase. Na této kartě můžete také konfigurovat oprávnění pro jednotlivé aplikace.
- Na kartě **Spuštěno při spuštění počítače** se zobrazuje seznam aplikací spouštěných při spuštění operačního systému.

Pravidla pro vytváření masek názvů pro soubory nebo složky

Maska názvu souboru nebo složky reprezentuje názvy složek nebo názvy a přípony souborů, v nichž jsou použity určité společné znaky.

K vytvoření masky názvu souboru nebo složky můžete použít následující běžné znaky:

- Znak `*` (hvězdička), který nahrazuje jakoukoli kombinaci znaků (včetně prázdné). Například maska `C:\*.txt` bude představovat všechny cesty k souborům s příponou `txt` umístěným ve složkách a podsložkách na jednotce (C:).
- Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.

Úprava šablon zpráv součásti Kontrola aplikací

Když se uživatel pokusí spustit nějakou aplikaci, která je blokovaná pravidlem součásti Kontrola aplikací, aplikace Kaspersky Endpoint Security zobrazí zprávu o tom, že spouštění aplikace je zablokováno. Pokud se uživatel domnívá, že spuštění dané aplikace bylo zablokováno omylem, může pomocí odkazu ve zprávě odeslat zprávu místnímu podnikovému správci sítě.

Pro zprávu, která se zobrazí při zablokování spuštění aplikace, a zprávu odesílanou správci jsou k dispozici speciální šablony. Tyto šablony zpráv můžete upravit.

Postup úpravy šablony zprávy:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Ochrana** → **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. V bloku **Šablony** nakonfigurujte šablony pro zprávy součásti Kontrola aplikací:
   - **Blokování**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.
   - **Zpráva správci**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.
4. Uložte změny.

Osvědčené postupy pro implementaci seznamu povolených aplikací

Při plánování zavedení seznamu povolených aplikací se doporučuje provést následující akce:

1. Vytvořte následující typy skupin:
   - Skupiny uživatelů. Skupiny uživatelů, pro které je třeba povolit použití různých sad aplikací.
   - Skupiny správy. Jedna nebo více skupin počítačů, na které aplikace Kaspersky Security Center použije seznam povolených aplikací. Pokud se pro tyto skupiny používají různá nastavení seznamu povolených aplikací, je nutné vytvořit více skupin počítačů.
2. Vytvořte seznam aplikací, jejichž spuštění musí být povoleno.

   Před vytvořením seznamu vám doporučujeme provést následující akce:

   a. Spusťte úlohu inventarizace.

      Informace o vytvoření, opakované konfiguraci a spuštění úlohy inventarizace jsou k dispozici v části Správa úloh.

   b. Zobrazte seznam spustitelných souborů.

Konfigurace režimu seznamu povolených položek pro aplikace

Při konfiguraci režimu seznamu povolených aplikací se doporučuje provést následující akce:

1. Vytvoření kategorií aplikací obsahujících aplikace, jejichž spuštění je nutné povolit.

Můžete vybrat jeden z následujících způsobů vytvoření kategorií aplikací:

- **Kategorie s ručně přidaným obsahem**. Do této kategorie můžete přidávat obsah ručně pomocí následujících podmínek:
  - Metadata souboru. Aplikace Kaspersky Security Center přidá do kategorie aplikace všechny spustitelné soubory doplněné o určená metadata.
  - Hodnota hash souboru. Aplikace Kaspersky Security Center přidá do kategorie aplikace všechny spustitelné soubory s určenou hodnotou hash.

    Použití této podmínky vyloučí možnost automatické instalace aktualizací, protože různé verze souborů budou mít jinou hodnotu hash.

  - Certifikát souboru. Aplikace Kaspersky Security Center přidá do kategorie aplikace všechny spustitelné soubory s určenou hodnotou hash.
  - Kategorie KL. Aplikace Kaspersky Security Center přidá do kategorie aplikace všechny aplikace, které jsou v zadané kategorii KL.
  - Cesta k aplikaci. Aplikace Kaspersky Security Center přidá do kategorie aplikace spustitelné soubory z této složky.

    Použití podmínky Application folder nemusí být bezpečné, protože bude povoleno spuštění jakékoli aplikace z určené složky. Pravidla, která používají kategorie aplikací s podmínkou Application folder, se doporučuje použít pouze na uživatele, u kterých je nutné povolit automatickou instalaci aktualizací.

- **Kategorie zahrnující spustitelné soubory z konkrétní složky**. Můžete určit složku, ze které budou spustitelné soubory automaticky přiřazeny k vytvořené kategorii aplikací.
- **Kategorie zahrnující spustitelné soubory z vybraných zařízení**. Můžete určit počítač, u kterého budou spustitelné soubory automaticky přiřazeny k vytvořené kategorii aplikací.

  Když použijete tento způsob vytvoření kategorií aplikací, aplikace Kaspersky Security Center obdrží informace o aplikacích v počítači ze složky **Spustitelné soubory**.

2. U součásti Kontrola aplikací vyberte režim seznamu povolených aplikací.
3. Pomocí vytvořených kategorií aplikací vytvořte pravidla součásti Kontrola aplikací.

Původně definovanými pravidly pro režim Seznam povolených položek je pravidlo **Golden Image** a pravidlo **Důvěryhodné nástroje aktualizace**. Tato pravidla součásti Kontrola aplikací odpovídají kategoriím KL. Kategorie KL „Golden Image“ obsahuje programy, které zajišťují normální činnost operačního systému. Kategorie KL „Důvěryhodné nástroje aktualizace“ obsahuje nástroje aktualizace nejrenomovanějších dodavatelů softwaru. Tato pravidla nelze odstranit. Nastavení těchto pravidel nelze upravit. Ve výchozím nastavení je pravidlo **Golden Image** povoleno a pravidlo **Důvěryhodné nástroje aktualizace** zakázáno. Všichni uživatelé mohou spouštět aplikace, které odpovídají podmínkám aktivace pro tato pravidla.

Golden Image

4. Určete aplikace, u kterých je nutné povolit automatickou instalaci aktualizací.

Automatickou instalaci aktualizací můžete povolit jedním z následujících způsobů:

- Povolením spuštění všech aplikací, které paří do libovolné kategorie KL, určete rozšířený seznam povolených aplikací.
- Povolením spuštění všech aplikací, které jsou podepsány certifikáty, určete rozšířený seznam povolených aplikací.

  Chcete-li povolit spuštění všech aplikací podepsaných certifikáty, můžete vytvořit kategorii s podmínkou na základě certifikátu, která použije pouze parametr **Předmět** s hodnotou *.
- U pravidla součásti Kontrola aplikací vyberte parametr **Důvěryhodné nástroje aktualizace**. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security vezme v potaz aplikace, které jsou zahrnuty v pravidlu jako důvěryhodné nástroje aktualizace. Aplikace Kaspersky Endpoint Security povolí spuštění aplikací, které byly nainstalovány nebo aktualizovány aplikacemi zahrnutými v pravidlu, za předpokladu, že se na tyto aplikace nevztahují žádná pravidla blokování.

  Při přenesení nastavení aplikace Kaspersky Endpoint Security je přenesen také seznam spustitelných souborů vytvořených důvěryhodnými nástroji aktualizace.
- Vytvořte složku a umístěte do ní spustitelné soubory aplikací, u kterých chcete povolit automatickou instalaci aktualizací. Poté vytvořte kategorii aplikací s podmínkou „Application folder“ a zadejte cestu této složce. Poté vytvořte pravidlo povolení a vyberte tuto kategorii.

  Použití podmínky Application folder nemusí být bezpečné, protože bude povoleno spuštění jakékoli aplikace z určené složky. Pravidla, která používají kategorie aplikací s podmínkou Application folder, se doporučuje použít pouze na uživatele, u kterých je nutné povolit automatickou instalaci aktualizací.

Testování režimu seznamu povolených položek

Aby pravidla součásti Kontrola aplikací neblokovala aplikace, jejichž provoz je vyžadovaný, doporučujeme povolit testování pravidel kontroly aplikací a analyzovat jejich funkci po vytvoření nových pravidel. Když je povoleno testování, aplikace Kaspersky Endpoint Security nebude blokovat aplikace, jejichž spouštění je zakázáno pravidly kontroly aplikací, ale místo toho odešle upozornění o jejich spuštění na administrační server.

Při testování režimu seznamu povolených aplikací se doporučuje provést následující akce:

1. Určení doby testování (v rozsahu od několika dnů do dvou měsíců)
2. Povolení testování pravidel součásti Kontrola aplikací
3. Zkontrolujte události vyplývající z testování funkce součásti Kontrola aplikací a zprávy o blokovaných aplikacích v testovacím režimu pro účely analýzy výsledků testování.
4. Na základě výsledků analýzy proveďte změny nastavení režimu seznamu povolených aplikací.

   Zejména můžete na základě výsledků testů do kategorie aplikací přidat spustitelné soubory související s událostmi.

Podpora režimu seznamu povolených položek

Po výběru akce blokování u součásti Kontrola aplikací se doporučuje dále podporovat režim seznamu povolených aplikací provedením následujících akcí:

- Zkontrolujte akce vyplývající z funkce součásti Kontrola aplikací a zprávy o blokovaných spuštěních pro účely analýzy účinnosti součásti Kontrola aplikací.
- Analyzujte žádosti uživatelů o přístup k aplikacím.
- Analyzujte neznámé spustitelné soubory kontrolou jejich reputace ve službě Kaspersky Security Network.
- Před instalací aktualizací operačního systému nebo softwaru nainstalujte tyto aktualizace v testovací skupině počítačů, abyste zkontrolovali, jak budou zpracovány pravidly kontroly aplikací.
- Přidejte nezbytné aplikace do kategorií použitých v pravidlech kontroly aplikací.

Monitorování síťových portů

Při použití aplikace Kaspersky Endpoint Security sledují součásti Kontrola webu, Ochrana před hrozbami v poště a Ochrana před webovými hrozbami datové toky, které jsou přenášené přes určité protokoly a prochází přes určité otevřené porty TCP a UDP v počítači uživatele. Například součást Ochrana před hrozbami v poště analyzuje informace přenášené přes protokol SMTP, zatímco součást Ochrana před webovými hrozbami analyzuje informace přenášené přes protokol HTTP a FTP.

Aplikace Kaspersky Endpoint Security dělí porty TCP a UDP počítače uživatele do několika skupin v závislosti na pravděpodobnosti jejich zneužití. Některé síťové porty jsou vyhrazeny pro zranitelné služby. Doporučujeme sledovat tyto porty důkladněji, protože je u nich větší pravděpodobnost, že na ně bude cílit síťový útok. Pokud používáte nestandardní služby využívající nestandardní síťové porty, tyto síťové porty se mohou stát cílem útočících počítačů. Můžete zadat seznam síťových portů a seznam aplikací, které vyžadují přístup k síti. Tyto porty a aplikace pak budou důkladněji sledovány součástmi Ochrana před hrozbami v poště a Ochrana před webovými hrozbami během sledování síťového provozu.

Povolení monitorování všech síťových portů

Postup povolení monitorování všech síťových portů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.
3. V části **Sledované porty** vyberte možnost **Sledovat všechny síťové porty**.
4. Uložte změny.

Vytvoření seznamu sledovaných síťových portů

Postup vytvoření seznamu sledovaných síťových portů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V části **Sledované porty** vyberte položku **Sledovat pouze vybrané síťové porty**.

4. Klikněte na tlačítko **Vybrat**.

   Tím otevřete seznam síťových portů, které se obvykle používají pro přenos e-mailů a síťový provoz. Tento seznam síťových portů je součástí balíčku Kaspersky Endpoint Security.

5. Pomocí přepínače ve sloupci **Stav** můžete povolit nebo zakázat monitorování síťových portů.

6. Pokud v seznamu síťových portů není uveden nějaký síťový port, můžete jej přidat podle následujících pokynů:

   a. Klikněte na tlačítko **Přidat**.

   b. V okně, které se otevře, zadejte číslo síťového portu a stručný popis.

   c. Pro monitorování síťových portů nastavte stav **Aktivní** nebo **Neaktivní**.

7. Uložte změny.

Pokud je protokol FTP používán v pasivním režimu, připojení lze vytvořit prostřednictvím náhodného síťového portu, který není přidaný na seznam sledovaných síťových portů. Chcete-li tato připojení chránit, povolte monitorování všech síťových portů nebo nakonfigurujte řízení síťových portů pro aplikace, které navazují připojení FTP.

Vytvoření seznamu aplikací, pro které jsou sledovány všechny síťové porty

Můžete vytvořit seznam aplikací, pro které aplikace Kaspersky Endpoint Security sleduje všechny síťové porty.

Do seznamu aplikací, pro které aplikace Kaspersky Endpoint Security sleduje všechny síťové porty, doporučujeme zahrnout aplikace, které přijímají nebo odesílají data prostřednictvím protokolu FTP.

Postup vytvoření seznamu aplikací, pro které jsou sledovány všechny síťové porty:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Nastavení sítě**.

3. V části **Sledované porty** vyberte položku **Sledovat pouze vybrané síťové porty**.

4. Zaškrtněte políčko **Sledovat všechny porty aplikací ze seznamu doporučeného společností Kaspersky**.

   Pokud je zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security sleduje všechny porty v případě následujících aplikací:

   - Adobe Reader,
   - Apple Application Support,
   - Google Chrome,

- Microsoft Edge,
- Mozilla Firefox,
- Internet Explorer,
- Java,
- mIRC,
- Opera,
- Pidgin,
- Safari,
- Mail.ru Agent,
- Yandex Browser.

5. Zaškrtněte políčko **Sledovat všechny porty u zadaných aplikací**.
6. Klikněte na tlačítko **Vybrat**.
   Tím otevřete seznam aplikací, pro které aplikace Kaspersky Endpoint Security monitoruje všechny síťové porty.
7. Pomocí přepínače ve sloupci **Stav** můžete povolit nebo zakázat monitorování síťových portů.
8. Pokud nějaká aplikace na seznamu aplikací není, přidejte ji podle těchto pokynů:
   a. Klikněte na tlačítko **Přidat**.
   b. V okně, které se otevře, zadejte cestu ke spustitelnému souboru aplikace a krátký popis.
   c. Pro monitorování síťových portů nastavte stav **Aktivní** nebo **Neaktivní**.
9. Uložte změny.

Export a import seznamů sledovaných portů

Aplikace Kaspersky Endpoint Security používá ke sledování síťových portů následující seznamy: seznam síťových portů a seznam aplikací, jejichž porty tato aplikace sleduje. Seznamy monitorovaných portů můžete exportovat do souboru XML. Poté můžete soubor upravit, například přidat velké množství portů se stejným popisem. Funkci exportu/importu můžete také použít k zálohování seznamů monitorovaných portů nebo k migraci seznamů na jiný server.

Jak exportovat a importovat seznamy monitorovaných portů v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Obecná nastavení** → **Nastavení sítě**.
6. V části **Sledované porty** vyberte položku **Sledovat pouze vybrané síťové porty**.
7. Klikněte na tlačítko **Nastavení**.

   Otevře se okno **Síťové porty**. V okně **Síťové porty** se zobrazí seznam síťových portů, které se obvykle používají pro přenos e-mailů a síťový provoz. Tento seznam síťových portů je součástí balíčku Kaspersky Endpoint Security.
8. Postup exportu seznamu síťových portů:
   a. V seznamu síťových portů vyberte porty, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.

      Pokud jste žádný port nevybrali, aplikace Kaspersky Endpoint Security exportuje všechny porty.
   b. Klikněte na tlačítko **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam síťových portů, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam síťových portů do souboru XML.
9. Postup exportu seznamu aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security:
   a. Zaškrtněte políčko **Sledovat všechny porty u zadaných aplikací**.
   b. V seznamu aplikací vyberte aplikace, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.

      Pokud jste žádnou aplikaci nevybrali, aplikace Kaspersky Endpoint Security exportuje všechny aplikace.
   c. Klikněte na tlačítko **Exportovat**.
   d. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam aplikací, a vyberte složku, do které chcete tento soubor uložit.
   e. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam aplikací do souboru XML.
10. Postup importu seznamu síťových portů:
    a. V seznamu síťových portů klikněte na tlačítko **Importovat**.

       V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam síťových portů.

b. Klikněte na tlačítko **Otevřít**.

Pokud počítač již seznam síťových portů obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

11. Postup importu seznamu aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security:

a. V seznamu aplikací klikněte na tlačítko **Importovat**.

V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam aplikací.

b. Klikněte na tlačítko **Otevřít**.

Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

12. Uložte změny.

[Jak exportovat a importovat seznamy monitorovaných sportů ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznamy monitorovaných portů.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Obecná nastavení** → **Nastavení sítě**.
5. Postup exportu seznamu síťových portů:

   a. V části **Sledované porty** vyberte položku **Sledovat pouze vybrané síťové porty**.

   b. Klikněte na odkaz **Vybráno N portů**.

   Otevře se okno **Síťové porty**. V okně **Síťové porty** se zobrazí seznam síťových portů, které se obvykle používají pro přenos e-mailů a síťový provoz. Tento seznam síťových portů je součástí balíčku Kaspersky Endpoint Security.

   c. V seznamu síťových portů vyberte porty, které chcete exportovat.

   d. Klikněte na tlačítko **Exportovat**.

   e. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam síťových portů, a vyberte složku, do které chcete tento soubor uložit.

   f. Klikněte na tlačítko **Uložit**.

   Aplikace Kaspersky Endpoint Security exportuje celý seznam síťových portů do souboru XML.
6. Postup exportu seznamu aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security:

   a. V bloku **Sledované porty** zaškrtněte políčko **Sledovat všechny porty u zadaných aplikací**.

   b. Klikněte na odkaz **Vybráno N aplikací**.

   c. V seznamu aplikací vyberte aplikace, které chcete exportovat.

   d. Klikněte na tlačítko **Exportovat**.

   e. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam aplikací, a vyberte složku, do které chcete tento soubor uložit.

   f. Klikněte na tlačítko **Uložit**.

   Aplikace Kaspersky Endpoint Security exportuje celý seznam aplikací do souboru XML.
7. Postup importu seznamu síťových portů:

   a. V seznamu síťových portů klikněte na tlačítko **Importovat**.

   V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam síťových portů.

   b. Klikněte na tlačítko **Otevřít**.

   Pokud počítač již seznam síťových portů obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

8. Postup importu seznamu aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security:

   a. V seznamu aplikací klikněte na tlačítko **Importovat**.

      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam aplikací.

   b. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

9. Uložte změny.

Managed Detection and Response

Do aplikace Kaspersky Endpoint Security verze 11.6.0 byla přidána součást Managed Detection and Response. Tato součást umožňuje interakci s řešením známým jako Kaspersky Managed Detection and Response. *Kaspersky Managed Detection and Response (MDR)* neustále hledá, detekuje a eliminuje hrozby cílící na vaši organizaci. Podrobné informace o tom, jak řešení funguje, *najdete v průvodci nápovědou k aplikaci Kaspersky Managed Detection and Response*.

Při interakci s řešením Kaspersky Managed Detection and Response vám aplikace umožňuje provádět následující funkce:

- Aktivovat součást Managed Detection and Response pomocí konfiguračního souboru BLOB.
- Provádět příkazy z řešení Kaspersky Managed Detection and Response.
- Odesílat telemetrická data do řešení Kaspersky Managed Detection and Response pro detekci hrozeb.

Integrace s řešením Kaspersky Managed Detection and Response

Integrace s řešením Kaspersky Managed Detection and Response sestává z následujících kroků:

1. **Konfigurace privátní služby Kaspersky Security Network**

   Pokud používáte cloudovou konzolu aplikace Kaspersky Security Center, tento krok přeskočte. Cloudová konzola aplikace Kaspersky Security Center automaticky konfiguruje místní síť Kaspersky Security Network při instalaci modulu plug-in MDR.

   Privátní KSN podporuje výměnu dat mezi počítači a dedikovanými servery služby Kaspersky Security Network, ale ne globální KSN.

   Nahrajte konfigurační soubor služby Kaspersky Security Network do vlastností serveru pro správu. Konfigurační soubor aplikace Kaspersky Security Network je umístěn v archivu ZIP konfiguračního souboru MDR. Archiv ZIP můžete získat v konzole aplikace Kaspersky Managed Detection and Response. Další informace o konfiguraci privátní KSN najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*. Konfigurační soubor služby Kaspersky Security Network můžete také nahrát do počítače z příkazového řádku (viz pokyny níže).

   Jak konfigurovat privátní KSN z příkazového řádku

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, kde se nachází distribuční balíček aplikace Kaspersky Endpoint Security.
3. Spusťte následující příkaz:

   ```
   avp.com KSN /private <název souboru>
   ```

   `<název souboru>` je název konfiguračního souboru obsahujícího nastavení privátní KSN (formát souboru PKCS7 nebo PEM).

   Příklad:

   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Aplikace Kaspersky Endpoint Security tak bude používat privátní KSN k určení reputace souborů, aplikací a webů. V nastavení zásad v části **Kaspersky Security Network** se zobrazí tento provozní stav: *Síť KSN: privátní KSN*.

Aby mohla součást Managed Detection and Response fungovat, musíte povolit rozšířený režim KSN.

2. **Aktivujte součást Managed Detection a Response.**

Načtěte konfigurační soubor BLOB do zásad Kaspersky Endpoint Security (viz pokyny níže). Soubor BLOB obsahuje ID klienta a informace o licenci pro řešení Kaspersky Managed Detection and Response. Soubor BLOB je umístěn uvnitř archivu ZIP konfiguračního souboru MDR. Archiv ZIP můžete získat v konzole aplikace Kaspersky Managed Detection and Response. Podrobné informace o souboru BLOB *najdete v průvodci nápovědou k řešení Kaspersky Managed Detection and Response*.

Jak aktivovat součást Managed Detection and Response v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte položky **Rozšiřování ochrany před hrozbami → Detekce a reakce**.
6. Zaškrtněte políčko **Managed Detection and Response**.
7. V bloku **Nastavení** klikněte na možnost **Importovat** a vyberte soubor BLOB obdržený v konzole aplikace Kaspersky Managed Detection and Response. Soubor má příponu P7.
8. Uložte změny.

Jak aktivovat součást Managed Detection and Response ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Rozšiřování ochrany před hrozbami** → **Detekce a reakce**.
5. Zapněte přepínač **Managed Detection and Response**.
6. Klikněte na tlačítko **Importovat** a vyberte soubor BLOB, který byl získán v konzole řešení Managed Detection and Response. Soubor má příponu P7.
7. Uložte změny.

Jak aktivovat součást Managed Detection and Response z příkazového řádku

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, kde se nachází distribuční balíček aplikace Kaspersky Endpoint Security.
3. Spusťte následující příkaz:

   - Pokud nastavení aplikace není chráněno heslem:

     `avp.com MDRLICENSE /ADD <název souboru>`

     `<Název souboru>` je název konfiguračního souboru BLOB pro aktivaci součásti Managed Detection and Response (formát souboru P7).

   - Pokud je nastavení aplikace chráněno heslem:

     `avp.com MDRLICENSE /ADD <název souboru> / login=<uživatelské jméno> /password=<heslo>`

Kaspersky Endpoint Security ověří soubor BLOB. Ověření souboru BLOB zahrnuje kontrolu digitálního podpisu a licenčního období. Pokud je soubor BLOB úspěšně ověřen, aplikace Kaspersky Endpoint Security soubor nahraje a odešle jej do počítače během další synchronizace s aplikací Kaspersky Security Center. Provozní stav součásti zkontrolujete zobrazením *zprávy o stavu součástí aplikace*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Managed Detection and Response** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Aby mohla součást Managed Detection and Response fungovat, musíte povolit následující součásti:

- Kaspersky Security Network (rozšířený režim).
- Detekce chování.

Povolení těchto součástí není volitelné. V opačném případě nemůže Kaspersky Managed Detection and Response fungovat, protože neobdrží potřebná telemetrická data.

Kromě toho používá Kaspersky Managed Detection and Response data obdržená z jiných součástí aplikace. Povolení těchto součástí je volitelné. Mezi součásti, které poskytují další data, patří:

- Ochrana před webovými hrozbami.
- Ochrana před hrozbami v poště.
- Brána firewall.

Migrace z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security pro systém Windows

Řešení MDR podporuje aplikace Kaspersky Endpoint Security verze 11 a novější. Kaspersky Endpoint Security verze 11–11.5.0 odesílá telemetrická data do řešení Kaspersky Managed Detection and Response za účelem zjišťování hrozeb. Kaspersky Endpoint Security verze 11.6.0 má všechny funkce integrovaného agenta (Kaspersky Endpoint Agent).

Pokud používáte aplikaci Kaspersky Endpoint Security 11–11.5.0, musíte pro práci s řešením aktualizovat databáze na nejnovější verzi. Musíte rovněž nainstalovat aplikaci Kaspersky Endpoint Agent.

Pokud používáte Kaspersky Endpoint Security 11.6.0 nebo novější, pro práci s řešením MDR musíte při instalaci aplikace vybrat součást Managed Detection and Response. V tomto případě není nutné instalovat aplikaci Kaspersky Endpoint Agent.

Postup migrace z aplikace Kaspersky Endpoint Agent na Kaspersky Endpoint Security pro systém Windows:

1. V zásadách aplikace Kaspersky Endpoint Security nakonfigurujte integraci s řešením Kaspersky Managed Detection and Response.
2. V zásadách aplikace Kaspersky Endpoint Agent zakažte součást Managed Detection and Response.

Pokud se zásady aplikace Kaspersky Endpoint Security vztahují i na počítače, na nichž není nainstalován aplikace Kaspersky Endpoint Security 11–11.5.0, musíte pro tyto počítače nejdříve vytvořit samostatné zásady aplikace Kaspersky Endpoint Agent. V nových zásadách nakonfigurujte integraci s řešením Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent podporuje interakci mezi aplikací a dalšími řešeními Kaspersky pro detekci pokročilých hrozeb (například Kaspersky Sandbox). Řešení společnosti Kaspersky jsou kompatibilní s konkrétními verzemi aplikace Kaspersky Endpoint Agent.

Úplné informace o aplikaci Kaspersky Endpoint Agent pro systém Windows obsažené v softwarovém řešení, které používáte, a úplné informace o samostatném řešení naleznete v příručce nápovědy k příslušnému produktu:

- *Průvodce nápovědou k platformě Kaspersky Anti Targeted Attack*
- *Průvodce nápovědou k aplikaci Kaspersky Sandbox*
- *Průvodce nápovědou k aplikaci Kaspersky Endpoint Detection and Response Optimum*
- *Průvodce nápovědou k aplikaci Kaspersky Managed Detection and Response*

Součástí distribuční sady aplikace Kaspersky Endpoint Security je Kaspersky Endpoint Agent. Aplikaci Kaspersky Endpoint Agent můžete nainstalovat během instalace aplikace Kaspersky Endpoint Security. Chcete-li tak učinit, musíte během instalace aplikace vybrat součást Endpoint Agent (například v instalačním balíčku). Po instalaci aplikace se součástí Endpoint Agent budou aplikace Kaspersky Endpoint Security a Kaspersky Endpoint Agent přidány na seznam nainstalovaných aplikací. Po odinstalování aplikace Kaspersky Endpoint Security bude automaticky odinstalována i součást Kaspersky Endpoint Agent.

Vymazat data

Aplikace Kaspersky Endpoint Security umožňuje využití úlohy, která vzdáleně odstraní data z počítačů uživatelů.

Aplikace Kaspersky Endpoint Security odstraní data následovně:

- v bezobslužném režimu;
- na pevných discích a vyměnitelných jednotkách;
- Pro všechny uživatelské účty v počítači.

Aplikace Kaspersky Endpoint Security spustí úlohu *Vymazat data* bez ohledu na to, který typ licence používáte, a to i po vypršení platnosti licence.

Režimy výmazu dat

Tato úloha umožňuje odstranit data v následujících režimech:

- Okamžité vymazání dat.

  V tomto režimu můžete například odstranit zastaralá data a uvolnit místo na disku.

- Odložené vymazání dat.

  Tento režim je určen například k ochraně dat na notebooku v případě ztráty nebo odcizení. Můžete nakonfigurovat automatické odstranění dat, pokud notebook překročí hranice podnikové sítě a nebyl dlouho synchronizován s aplikací Kaspersky Security Center.

Plán pro výmaz dat nelze nastavit ve vlastnostech úlohy. Data lze odstranit pouze okamžitě po ručním spuštění úlohy, nebo můžete nakonfigurovat odložený výmaz dat, pokud chybí spojení s aplikací Kaspersky Security Center.

Omezení

Výmaz dat má následující omezení:

- Úlohu *Vymazání dat* může spravovat pouze správce aplikace Kaspersky Security Center. Úlohu nelze nakonfigurovat ani spustit v místním rozhraní aplikace Kaspersky Endpoint Security.
- U souborového systému NTFS aplikace Kaspersky Endpoint Security odstraní pouze názvy hlavních datových proudů. Názvy alternativních datových proudů nelze odstranit.
- Když odstraníte soubor symbolického odkazu, aplikace Kaspersky Endpoint Security odstraní i soubory, u nichž jsou v tomto symbolickém odkazu uvedeny cesty k nim.

Vytvoření úlohy Vymazat data

Odstranění dat v počítačích uživatelů:

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   b. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Vymazat data**.

   c. Do pole **Název úlohy** zadejte krátký popis, například `Vymazat data (proti krádeži)`.

   d. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Další**.

   Pokud jsou v rámci rozsahu úlohy přidány do skupiny pro správu nové počítače, je v těchto nových počítačích spuštěna úloha okamžitého odstranění dat pouze v případě, že je úloha dokončena do 5 minut od přidání těchto počítačů.

5. Kliknutím na tlačítko **Dokončit** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

6. Klikněte na úlohu **Vymazat data** aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

7. Vyberte kartu **Nastavení aplikace**.

8. Vyberte způsob odstranění dat:

   - **Odstranit pomocí operačního systému**. Aplikace Kaspersky Endpoint Security používá prostředky operačního systému k odstranění souborů bez jejich odeslání do koše.
   - **Odstranit úplně, bez možnosti obnovení**. Aplikace Kaspersky Endpoint Security přepíše soubory náhodnými daty. Po vymazání je prakticky nemožné obnovit data.

9. Pokud chcete odstranění dat odložit, zaškrtněte políčko **Automaticky odstranit data, pokud nedojde po více než N dní k připojení k aplikaci Kaspersky Security Center**. Zadejte počet dní.

   Úloha odloženého odstranění dat bude provedena pokaždé, když po definovanou dobu nedojde k připojení k aplikaci Kaspersky Security Center.

   Při konfiguraci odloženého odstranění dat nezapomeňte, že zaměstnanci mohou vypnout svůj počítač před odjezdem na dovolenou. V takovém případě může být překročena doba, po níž se počítač nepřipojí, a data budou odstraněna. Zvažte také pracovní harmonogram offline uživatelů. Podrobnější informace o práci s počítači v režimu offline a s uživateli mimo kancelář *najdete v nápovědě k aplikaci Kaspersky Security Center*.

   Jestliže toto políčko není zaškrtnuté, bude úloha provedena ihned po synchronizaci s aplikací Kaspersky Security Center.

10. Vytvoření seznamu objektů k odstranění:

    - **Složky**. Aplikace Kaspersky Endpoint Security odstraní všechny soubory ve složce a její podsložky. Aplikace Kaspersky Endpoint Security nepodporuje pro zadání cesty ke složce masky ani proměnné prostředí.
    - **Soubory podle přípony**. Aplikace Kaspersky Endpoint Security vyhledá soubory se zadanými příponami na všech jednotkách počítače, včetně vyměnitelných jednotek. Pomocí znaku „`;`“ nebo „`,`“ zadejte více přípon.
    - **Předdefinované složky**. Aplikace Kaspersky Endpoint Security odstraní soubory z následujících oblastí:
        - **Dokumenty**. Soubory ve standardní systémové složce *Dokumenty* a jejích podsložkách.
        - **Soubory cookie**. Soubory, ve kterých prohlížeč ukládá data z webových stránek navštívených uživatelem (například údaje o autorizaci uživatele).
        - **Plocha**. Soubory ve standardní systémové složce *Plocha* a jejích podsložkách.
        - **Dočasné soubory aplikace Internet Explorer**. Dočasné soubory související s provozem aplikace Internet Explorer, jako jsou kopie webových stránek, obrázky a mediální soubory.
        - **Dočasné soubory**. Dočasné soubory související s provozováním aplikací nainstalovaných v počítači. Například aplikace sady Microsoft Office vytvářejí dočasné soubory obsahující záložní kopie dokumentů.
        - **Soubory aplikace Outlook**. Soubory související s provozem poštovního klienta aplikace Outlook: datové soubory (PST), offline datové soubory (OST), offline soubory adresáře (OAB) a soubory osobních adresářů (PAB).
        - **Profil uživatele**. Sada souborů a složek, v nichž je uloženo nastavení operačního systému pro místní uživatelský účet.

    Na každé kartě můžete vytvořit seznam objektů, které chcete odstranit. Aplikace Kaspersky Endpoint Security vytvoří konsolidovaný seznam a po dokončení úlohy odstraní soubory z tohoto seznamu.

    Soubory, které jsou nutné pro provoz aplikace Kaspersky Endpoint Security, nelze odstranit.

11. Klikněte na tlačítko **Uložit**.
12. Zaškrtněte políčko vedle úlohy.
13. Klikněte na tlačítko **Spustit**.

    V počítačích uživatelů budou smazána data podle zvoleného režimu: okamžitě nebo v případě, kdy nedojde k připojení. Pokud aplikace Kaspersky Endpoint Security nemůže soubor odstranit, například když uživatel soubor aktuálně používá, nepokusí se jej znovu odstranit. Chcete-li dokončit odstranění dat, spusťte úlohu znovu.

Ochrana heslem

Počítač může sdílet více uživatelů s různou úrovní počítačové gramotnosti. Pokud mají uživatelé neomezený přístup k aplikaci Kaspersky Endpoint Security a jejím nastavením, celková úroveň ochrany počítače může být snížena. Ochrana heslem umožňuje omezit přístup uživatelů k aplikaci Kaspersky Endpoint Security podle oprávnění, která jsou jim udělena (například oprávnění k ukončení aplikace).

Pokud má uživatel, který zahájil relaci systému Windows (*uživatel relace*), oprávnění provést akci, aplikace Kaspersky Endpoint Security nepožaduje uživatelské jméno a heslo ani dočasné heslo. Uživatel získá přístup do aplikace Kaspersky Endpoint Security v souladu s udělenými oprávněními.

Pokud uživatel relace nemá oprávnění k provedení akce, může získat přístup k aplikaci následujícími způsoby:

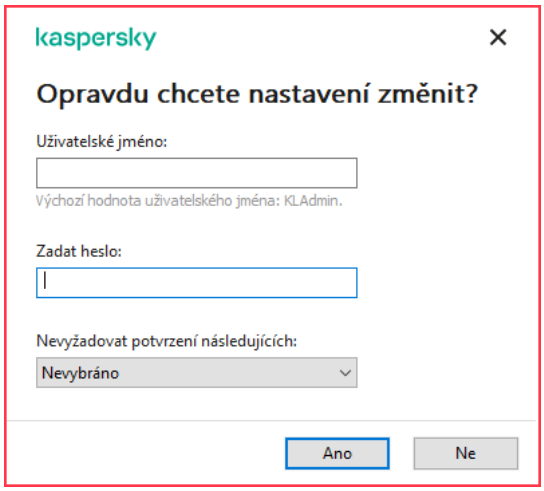
- Zadejte uživatelské jméno a heslo.

  Tento způsob je vhodný pro každodenní činnosti. Chcete-li provést akci chráněnou heslem, musíte zadat přihlašovací údaje účtu domény uživatele s požadovaným oprávněním. V tomto případě musí být počítač v této doméně. Pokud počítač v dané doméně není, můžete použít účet KLAdmin.

- Zadejte dočasné heslo.

  Tento způsob je vhodný k udělení dočasných oprávnění za účelem provedení blokovaných akcí (například ukončení aplikace) uživatelům mimo podnikovou síť. Když vyprší platnost dočasného hesla nebo skončí relace, aplikace Kaspersky Endpoint Security vrátí svá nastavení do předchozího stavu.

Když se uživatel pokusí provést akci chráněnou heslem, aplikace Kaspersky Endpoint Security vyzve uživatele k zadání uživatelského jména a hesla nebo dočasného hesla (viz obrázek níže).



Výzva k zadání hesla za účelem přístupu k aplikaci Kaspersky Endpoint Security

Uživatelské jméno a heslo

Chcete-li získat přístup k aplikaci Kaspersky Endpoint Security, je nutné zadat přihlašovací údaje k účtu domény. Ochrana heslem podporuje následující účty:

- **KLAdmin**. Účet správce s neomezeným přístupem k aplikaci Kaspersky Endpoint Security. Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem. Oprávnění k účtu KLAdmin nelze odvolat. Když povolíte ochranu heslem, aplikace Kaspersky Endpoint Security vás vyzve k nastavení hesla k účtu KLAdmin.

- **Skupina Všichni**. Integrovaná skupina systému Windows, která zahrnuje všechny uživatele v podnikové síti. Uživatelé ve skupině Všichni mohou přistupovat k aplikaci podle oprávnění, která jsou jim udělena.

- **Jednotliví uživatelé nebo skupiny**. Uživatelské účty, u kterých můžete nakonfigurovat jednotlivá oprávnění. Pokud je například akce zablokována pro skupinu Všichni, můžete tuto akci povolit pro jednotlivého uživatele nebo skupinu.

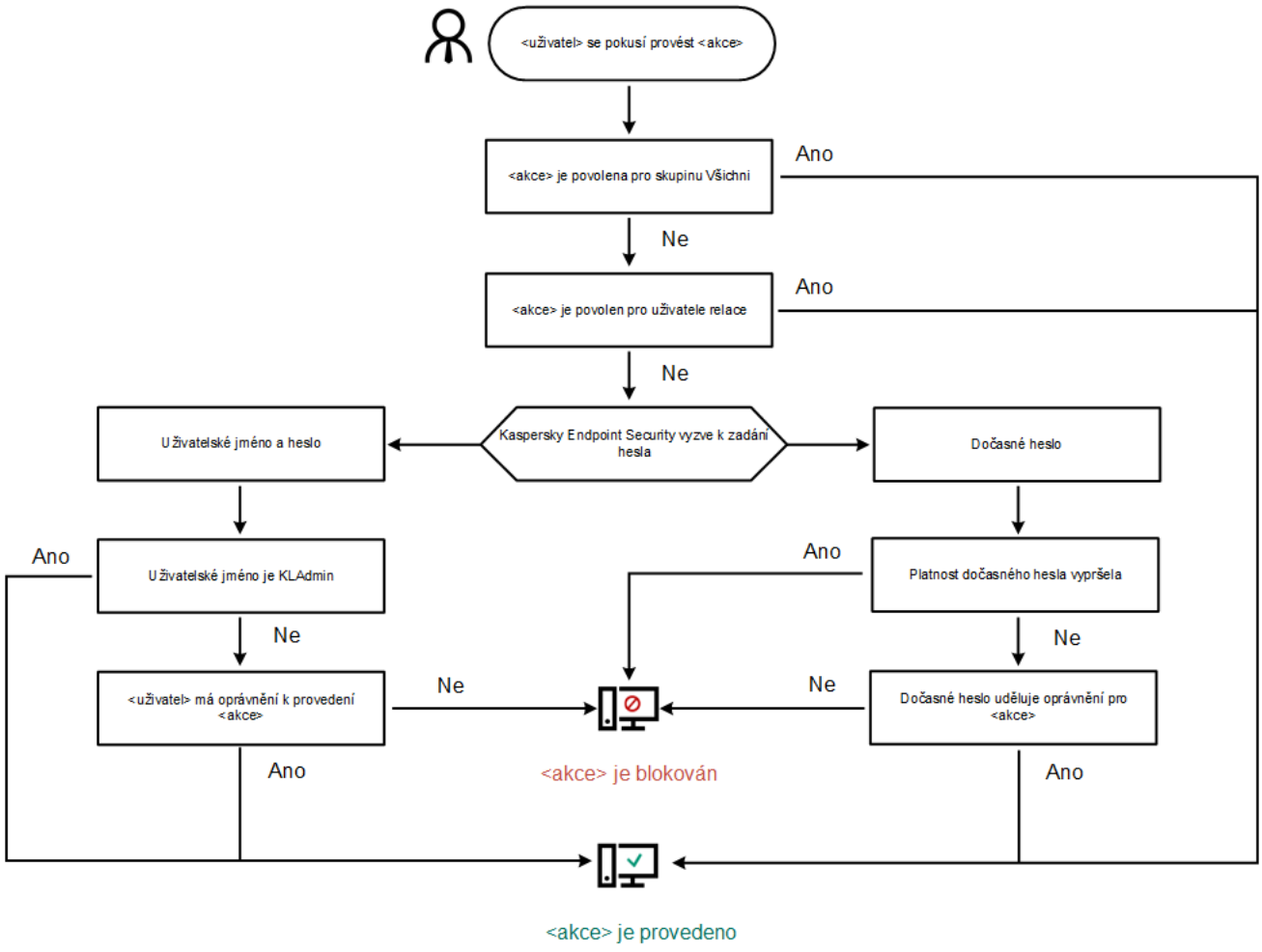
- **Uživatel relace**. Účet uživatele, který spustil relaci systému Windows. Když se zobrazí výzva k zadání hesla, můžete přepnout na jiného uživatele relace (zaškrtávací políčko **Uložit heslo pro aktuální relaci**). V tomto případě aplikace Kaspersky Endpoint Security považuje uživatele, jehož přihlašovací údaje účtu byly zadány, za uživatele relace a nikoli za uživatele, který spustil relaci systému Windows.

Dočasné heslo

Pomocí dočasného hesla lze udělit dočasný přístup k aplikaci Kaspersky Endpoint Security jednotlivému počítači mimo podnikovou síť. Správce vygeneruje dočasné heslo pro jednotlivý počítač ve vlastnostech počítače v aplikaci Kaspersky Security Center. Správce vybere akce, které budou chráněny dočasným heslem, a určí dobu platnosti dočasného hesla.

Algoritmus činnosti ochrany heslem

Aplikace Kaspersky Endpoint Security určí, zda povolit nebo blokovat akci chráněnou heslem, na základě následujícího algoritmu (viz obrázek níže).



Algoritmus činnosti ochrany heslem

Povolit ochranu heslem

Ochrana heslem umožňuje omezit přístup uživatelů k aplikaci Kaspersky Endpoint Security podle oprávnění, která jsou jim udělena (například oprávnění k ukončení aplikace).

Postup povolení ochrany heslem:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

   V okně s nastavením aplikace vyberte část **Rozhraní**.

2. Pomocí přepínače **Ochrana heslem** povolte nebo zakažte příslušnou součást.

3. Zadejte heslo k účtu KLAdmin a potvrďte jej.

   Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem.

   Pokud počítač používá nějaké zásady, správce může resetovat heslo k účtu KLAdmin ve vlastnostech zásad. Pokud počítač není připojen k aplikaci Kaspersky Security Center a zapomněli jste heslo k účtu KLAdmin, heslo není možné obnovit.

4. Nastavení oprávnění pro všechny uživatele v podnikové síti:

   a. V tabulce **Povolení** kliknutím na tlačítko **Upravit** otevřete seznam oprávnění pro skupinu uživatelů Všichni.

      Skupina uživatelů Všichni je integrovaná skupina systému Windows, která zahrnuje všechny uživatele v podnikové síti.

   b. Zaškrtněte políčka vedle akcí, které budou uživatelé moci provést bez zadání hesla.

      Pokud políčko není zaškrtnuto, uživatelům je zakázáno akci provést. Pokud například není zaškrtnuto políčko vedle oprávnění **Ukončit aplikaci**, můžete aplikaci ukončit pouze v případě, že jste přihlášeni jako uživatel KLAdmin nebo jako jednotlivý uživatel, který má požadované oprávnění, případně pokud zadáte dočasné heslo.

      Oprávnění týkající se ochrany heslem mají některé důležité aspekty, které je třeba zvážit. Přesvědčte se, zda jsou splněny všechny podmínky pro přístup k aplikaci Kaspersky Endpoint Security.

   c. Klikněte na tlačítko **OK**.

5. Uložte změny.

Když je povolena ochrana heslem, aplikace omezí přístup uživatelů k aplikaci Kaspersky Endpoint Security podle oprávnění udělených skupině Všichni. Akce, které jsou pro skupinu Všichni zakázány můžete provést pouze v případě, že použijete účet KLAdmin, jiný účet, kterému jsou udělena požadovaná oprávnění, případně pokud zadáte dočasné heslo.

Ochranu heslem můžete zakázat, pouze pokud jste přihlášeni jako KLAdmin. Ochranu heslem není možné zakázat, pokud používáte jiný uživatelský účet nebo dočasné heslo.

Během kontroly hesla můžete zaškrtnout políčko **Uložit heslo pro aktuální relaci**. V tomto případě aplikace Kaspersky Endpoint Security nezobrazí výzvu k zadání hesla, když se uživatel během doby trvání relace pokusí provést jinou akci chráněnou heslem.

Udělení oprávnění jednotlivým uživatelům nebo skupinám

Můžete udělit přístup k aplikaci Kaspersky Endpoint Security jednotlivým uživatelům nebo skupinám. Pokud je například ukončení aplikace zakázáno pro skupinu Všichni, můžete jednotlivému uživateli udělit oprávnění **Ukončit aplikaci**. V důsledku toho můžete ukončit aplikaci pouze v případě, že jste přihlášeni jako tento uživatel nebo jako KLAdmin.

Přihlašovací údaje k účtu můžete použít k přístupu k aplikaci pouze v případě, že je počítač v dané doméně. Pokud počítač v dané doméně není, můžete použít účet KLAdmin nebo dočasné heslo.

Postup udělení oprávnění jednotlivým uživatelům nebo skupinám:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

   V okně s nastavením aplikace vyberte část **Rozhraní**.

2. V tabulce **Ochrana heslem** klikněte na tlačítko **Přidat**.

3. V okně, které se otevře, klikněte na tlačítko **Vybrat uživatele**.

   Otevře se standardní dialogové okno Vyberte uživatele nebo skupiny.

4. Vyberte uživatele nebo skupinu ve službě Active Directory a potvrďte výběr.

5. V seznamu **Povolení** zaškrtněte políčka vedle akcí, které bude moci vybraný uživatel nebo vybraná skupina provést, aniž by se zobrazila výzva k zadání hesla.

   Pokud políčko není zaškrtnuto, uživatelům je zakázáno akci provést. Pokud například není zaškrtnuto políčko vedle oprávnění **Ukončit aplikaci**, můžete aplikaci ukončit pouze v případě, že jste přihlášeni jako uživatel KLAdmin nebo jako jednotlivý uživatel, který má požadované oprávnění, případně pokud zadáte dočasné heslo.

   Oprávnění týkající se ochrany heslem mají některé důležité aspekty, které je třeba zvážit. Přesvědčte se, zda jsou splněny všechny podmínky pro přístup k aplikaci Kaspersky Endpoint Security.

6. Uložte změny.

Pokud je tedy u skupiny Všichni omezen přístup k aplikaci, uživatelům budou udělena oprávnění pro přístup k aplikaci Kaspersky Endpoint Security podle jednotlivých oprávnění uživatelů.

Použití dočasného hesla k udělení oprávnění

Pomocí dočasného hesla lze udělit dočasný přístup k aplikaci Kaspersky Endpoint Security jednotlivému počítači mimo podnikovou síť. To je nezbytné k tomu, aby bylo uživateli povoleno provést blokovanou akci bez nutnosti získání přihlašovacích údajů účtu KLAdmin. Chcete-li použít dočasné heslo, počítač je nutné přidat do aplikace Kaspersky Security Center.

Povolení uživateli provedení blokované akce pomocí dočasného hesla:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Devices**.

4. Dvojitým kliknutím otevřete okno vlastností počítače.

5. V okně vlastností počítače vyberte část **Applications**.

6. V seznamu aplikací společnosti Kaspersky, které jsou nainstalovány v počítači, vyberte možnost **Kaspersky Endpoint Security pro systém Windows** a dvojitým kliknutím otevřete vlastnosti aplikace.

7. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.

8. V části **Ochrana heslem** klikněte na tlačítko **Nastavení**.

   Otevře se okno **Ochrana heslem**.

9. V části **Dočasné heslo** klikněte na tlačítko **Nastavení**.

   Otevře se okno **Vytvořit dočasné heslo**.

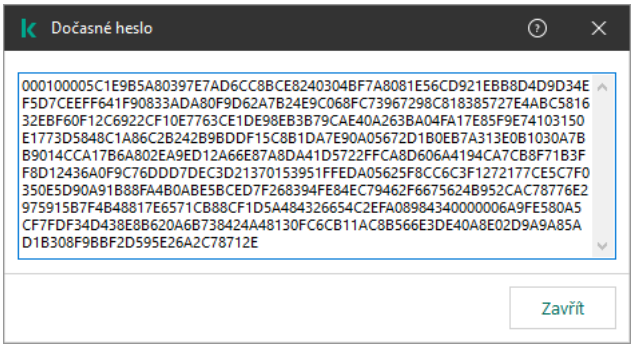
10. V poli **Datum vypršení platnosti** zadejte datum vypršení platnosti dočasného hesla.

11. V tabulce **Rozsah dočasného hesla** zaškrtněte políčka vedle akcí, které bude mít uživatel k dispozici po zadání dočasného hesla.

12. Klikněte na tlačítko **Vytvořit**.

    Otevře se okno obsahující dočasné heslo (viz obrázek níže).

13. Zkopírujte heslo a poskytněte jej uživateli.



Dočasné heslo

Zvláštní aspekty oprávnění týkajících se ochrany heslem

Oprávnění týkající se ochrany heslem mají některé důležité aspekty a omezení, které je třeba zvážit.

Konfigurovat nastavení aplikace

Pokud počítač uživatele používá nějaké zásady, přesvědčte se, zda jsou všechna požadovaná nastavení v zásadách zpřístupněna pro úpravy (jsou otevřeny atributy).

Ukončit aplikaci

Neexistují žádné zvláštní požadavky nebo omezení.

Zakázat součásti ochrany

- Není možné udělit oprávnění k deaktivaci součástí ochrany pro skupinu Všichni. Chcete-li povolit zakazování součástí ochrany jiným uživatelům než KLAdmin, přidejte uživatele nebo skupinu, který má v nastavení ochrany heslem oprávnění **Zakázat součásti ochrany**.
- Pokud počítač uživatele používá nějaké zásady, přesvědčte se, zda jsou všechna požadovaná nastavení v zásadách zpřístupněna pro úpravy (jsou otevřeny atributy).
- Aby bylo možné zakázat součásti ochrany v nastaveních aplikace, uživatel musí mít oprávnění **Konfigurovat nastavení aplikace**.
- Aby bylo možné zakázat součásti ochrany z místní nabídky (pomocí položky nabídky **Pozastavit ochranu**), uživatel musí mít kromě oprávnění **Zakázat součásti ochrany** také oprávnění **Zakázat součásti kontroly**.

Zakázat součásti kontroly

- Není možné udělit oprávnění k deaktivaci součástí kontroly pro skupinu Všichni. Chcete-li povolit zakazování součástí kontroly jiným uživatelům než KLAdmin, přidejte uživatele nebo skupinu, který má v nastavení ochrany heslem oprávnění **Zakázat součásti kontroly**.
- Pokud počítač uživatele používá nějaké zásady, přesvědčte se, zda jsou všechna požadovaná nastavení v zásadách zpřístupněna pro úpravy (jsou otevřeny atributy).
- Aby bylo možné zakázat součásti kontroly v nastaveních aplikace, uživatel musí mít oprávnění **Konfigurovat nastavení aplikace**.
- Aby bylo možné zakázat součásti kontroly z místní nabídky (pomocí položky nabídky **Pozastavit ochranu**), uživatel musí mít kromě oprávnění **Zakázat součásti kontroly** také oprávnění **Zakázat součásti ochrany**.

Zakázat zásadu aplikace Kaspersky Security Center

Skupině „Všichni“ nelze udělit oprávnění k deaktivaci zásad aplikace Kaspersky Security Center. Chcete-li povolit zakazování zásad jiným uživatelům než KLAdmin, přidejte uživatele nebo skupinu s oprávněním **Zakázat zásadu aplikace Kaspersky Security Center** v nastaveních ochrany heslem.

Odstranit klíč

Neexistují žádné zvláštní požadavky nebo omezení.

Odebrat/změnit/obnovit aplikaci

Pokud jste povolili odebrání, úpravy a obnovení aplikace u skupiny „Všichni“, aplikace Kaspersky Endpoint Security nežádá o heslo, když se uživatel pokusí o provedení těchto operací. Tuto aplikaci tak může instalovat, upravovat nebo obnovit jakýkoli uživatel včetně uživatelů mimo příslušnou doménu.

Obnovit přístup k datům na šifrovaných discích

Přístup k datům na šifrovaných discích můžete obnovit pouze v případě, že jste přihlášeni jako KLAdmin. Oprávnění k provedení této akce nelze udělit žádnému jinému uživateli.

Zobrazení sestav

Neexistují žádné zvláštní požadavky nebo omezení.

Obnovit ze zálohy

Neexistují žádné zvláštní požadavky nebo omezení.

Důvěryhodná zóna

Důvěryhodná zóna je správcem konfigurovaný seznam objektů a aplikací, které aplikace Kaspersky Endpoint Security nesleduje, když jsou aktivní.

Správce vytvoří důvěryhodnou zónou nezávisle a bere v potaz funkce objektů, které jsou zpracovávány, a aplikací nainstalovaných v počítači. Zahrnutí objektů a aplikací do důvěryhodné zóny může být vyžadováno v případech, kdy aplikace Kaspersky Endpoint Security zablokuje přístup k určitému objektu nebo aplikaci, ale vy jste si jisti, že daný objekt nebo aplikace jsou neškodné. Správce může také uživateli umožnit vytvoření vlastní místní důvěryhodné zóny pro konkrétní počítač. Tímto způsobem mohou uživatelé kromě obecné důvěryhodné zóny v zásadách vytvářet také vlastní místní seznamy výjimek a důvěryhodných aplikací.

Vytvoření výjimky z kontroly

Výjimka z kontroly je sada podmínek, které je nutné splnit, aby aplikace Kaspersky Endpoint Security nekontrolovala určitý objekt na přítomnost virů nebo jiných hrozeb.

Výjimky z kontroly umožňují bezpečně používat legitimní software, který může být pachateli využit k poškození počítače nebo data uživatele. I když tyto aplikace nemají žádnou škodlivou funkci, mohou být zneužity útočníky. Podrobnosti o legitimním softwaru, který může být využíván pachateli k poškození počítače nebo osobních údajů uživatele, najdete na webových stránkách encyklopedie IT Kaspersky.

Tyto aplikace mohou být aplikací Kaspersky Endpoint Security zablokovány. Pokud tyto aplikace blokovat nechcete, můžete pro ně nakonfigurovat výjimky z kontroly. To lze provést tak, že přidáte název nebo masku názvu uvedené v encyklopedii IT Kaspersky do důvěryhodné zóny. Například často používáte aplikaci Radmin ke vzdálené správě počítačů. Aplikace Kaspersky Endpoint Security vyhodnocuje tuto činnost jako podezřelou a může ji zablokovat. Aby tato aplikace nemohla být zablokována, vytvořte výjimku z kontroly za použití názvu nebo masky názvu, které jsou uvedené v encyklopedii IT Kaspersky.

Je-li ve vašem počítači nainstalována aplikace shromažďující a odesílající informace ke zpracování, aplikace Kaspersky Endpoint Security může tuto aplikaci klasifikovat jako malware. Aby k tomu nedošlo, můžete tuto aplikaci vyloučit z kontroly nakonfigurováním aplikace Kaspersky Total Security podle postupu uvedeného v tomto dokumentu.

Výjimky z kontroly mohou být použity následujícími součástmi a úlohami aplikace, které jsou nakonfigurovány správcem systému:

- Detekce chování.
- Prevence zneužití.
- Prevence narušení hostitele.
- Ochrana před souborovými hrozbami.
- Ochrana před webovými hrozbami.
- Ochrana před hrozbami v poště.
- Úlohy kontroly.

Aplikace Kaspersky Endpoint Security nekontroluje objekt, jestliže na začátku jedné z úloh kontroly přidáte jednotku nebo složku obsahující daný objekt do rozsahu kontroly. Výjimka z kontroly se však nepoužije, jestliže spustíte pro tento konkrétní objekt úlohu vlastní kontroly.

Jak vytvořit výjimku z kontroly v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V okně zásad vyberte možnosti **Obecná nastavení** → **Výjimky**.

6. V části **Výjimky z kontroly a důvěryhodné aplikace** klikněte na tlačítko **Nastavení**.

7. V okně **Důvěryhodná zóna** vyberte kartu **Výjimky z kontroly**.

   Otevře se okno obsahující seznam výjimek z kontroly.

8. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy výjimek v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Výjimky z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna ani odstranění výjimky v nadřazené zásadě nejsou možné.

9. Pokud chcete uživateli umožnit vytvoření místního seznamu výjimek, zaškrtněte políčko **Povolit používání místních výjimek**. Tímto způsobem může uživatel kromě obecného seznamu výjimek z kontroly generovaného v zásadách vytvořit svůj vlastní místní seznam výjimek z kontroly. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu výjimek z kontroly generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené soubory z kontroly.

10. Klikněte na tlačítko **Přidat**.

11. Postup vyloučení souboru nebo složky z kontroly:

    a. V části **Vlastnosti** zaškrtněte políčko **Soubor nebo složka**.

    b. Kliknutím na odkaz **Vybrat soubor nebo složku** v části **Popis výjimky pro sken** otevřete okno **Název souboru nebo složky**.

    c. Zadejte název souboru nebo složky nebo masku názvu souboru nebo složky, případně vyberte soubor nebo složku ve stromu složek po kliknutí na tlačítko **Procházet**.

       použitím masek:

       - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.

       - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složce s názvem `Složka`

a jejích podložkách. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.

- Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.

d. V okně **Název souboru nebo složky** klikněte na tlačítko **OK**.

V části **Popis výjimky z kontroly** okna **Výjimka z kontroly** se objeví odkaz na přidaný soubor nebo složku.

12. Postup vyloučení objektů určitého názvu z kontroly:

a. V části **Vlastnosti** zaškrtněte políčko **Název objektu**.

b. Kliknutím na odkaz **Zadejte název objektu** v části **Popis výjimky pro sken** otevřete okno **Název objektu**.

c. Zadejte název typu objektu podle klasifikace encyklopedie Kaspersky (například `Email-Worm`, `Rootkit` nebo `RemoteAdmin`).

Můžete použít masky se znakem `?` (nahradí libovolný jeden znak) a znakem `*` (nahradí libovolný počet znaků). Je-li například zadána maska `Client*`, aplikace Kaspersky Endpoint Security vyloučí z kontroly objekty `Client-IRC`, `Client-P2P` a `Client-SMTP`.

d. Klikněte na tlačítko **OK** v okně **Název objektu**.

V části **Popis výjimky z kontroly** okna **Výjimka z kontroly** se objeví odkaz na přidaný název objektu.

13. Pokud chcete z kontroly vyloučit jednotlivý soubor:

a. V části **Vlastnosti** zaškrtněte políčko **Hodnota hash objektu**.

b. Kliknutím na odkaz pro zadání hodnoty hash objektu otevřete okno **Hodnota hash objektu**.

c. Zadejte hodnotu hash souboru nebo vyberte požadovaný soubor po kliknutí na tlačítko **Procházet**.

V případě změny soubory se změní také hodnota hash souboru. V tomto případě nebude upravený soubor přidán k výjimkám.

d. V okně **Hodnota hash objektu** klikněte na tlačítko **OK**.

V části **Popis výjimky z kontroly** okna **Výjimka z kontroly** se objeví odkaz na přidaný objekt.

14. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

15. Určete, které součásti aplikace Kaspersky Endpoint Security mají výjimku z kontroly použít:

a. Kliknutím na **jakýkoli** odkaz v části **Popis výjimky pro sken** aktivujte odkaz **Vyberte komponenty**.

b. Kliknutím na odkaz **Vyberte komponenty** otevřete okno **Součásti ochrany**.

c. Zaškrtněte políčka vedle součástí, u kterých se má výjimka z kontroly použít.

d. V okně **Součásti ochrany** klikněte na tlačítko **OK**.

Když jsou v nastavení výjimky z kontroly zadány součásti, tato výjimka se použije jen během kontrol prováděných pomocí těchto zadaných součástí aplikace Kaspersky Endpoint Security.

Jestliže v nastavení výjimky z kontroly nejsou zadány žádné součásti, tato výjimka se použije během kontrol prováděných každou součástí aplikace Kaspersky Endpoint Security.

16. Pomocí zaškrtávacího políčka můžete výjimku kdykoli ukončit.

17. Uložte změny.

Jak vytvořit výjimku z kontroly ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete přidat výjimku.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Obecná nastavení** → **Výjimky**.
5. V bloku **Výjimky z kontroly a důvěryhodné aplikace** klikněte na odkaz **Výjimky z kontroly**.
6. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy výjimek v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Výjimky z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna ani odstranění výjimky v nadřazené zásadě nejsou možné.
7. Pokud chcete uživateli umožnit vytvoření místního seznamu výjimek, zaškrtněte políčko **Povolit používání místních výjimek**. Tímto způsobem může uživatel kromě obecného seznamu výjimek z kontroly generovaného v zásadách vytvořit svůj vlastní místní seznam výjimek z kontroly. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu výjimek z kontroly generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené soubory z kontroly.
8. Klikněte na tlačítko **Přidat**.
9. Vyberte, jak chcete výjimku přidat: **Soubor nebo složka**, **Název objektu** nebo **Hodnota hash objektu**.
10. Pokud chcete z kontroly vyloučit soubor nebo složku, vyberte je po kliknutí na tlačítko **Procházet**.

    Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky * a ?.

    - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
    - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složce s názvem `Složka` a jejích podložkách. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.
    - Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.
11. Chcete-li z kontroly vyloučit určitý typ objektu, zadejte do pole **Objekt** název typu objektu podle klasifikace encyklopedie Kaspersky (například `Email-Worm`, `Rootkit` nebo `RemoteAdmin`).

Můžete použít masky se znakem `?` (nahradí libovolný jeden znak) a znakem `*` (nahradí libovolný počet znaků). Je-li například zadána maska `Client*`, aplikace Kaspersky Endpoint Security vyloučí z kontroly objekty `Client-IRC`, `Client-P2P` a `Client-SMTP`.

12. Chcete-li z kontroly vyloučit jednotlivý soubor, do pole **Hodnota hash souboru** zadejte hodnotu hash tohoto souboru.

    V případě změny soubory se změní také hodnota hash souboru. V tomto případě nebude upravený soubor přidán k výjimkám.

13. V bloku **Součásti ochrany** vyberte součásti, pro které chcete výjimky z kontroly použít.

14. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

15. Pomocí přepínače můžete výjimku kdykoli ukončit.

16. Uložte změny.

Jak vytvořit výjimku z kontroly v rozhraní aplikace

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.
4. Klikněte na tlačítko **Přidat**.
5. Pokud chcete z kontroly vyloučit soubor nebo složku, vyberte je po kliknutí na tlačítko **Procházet**.

   Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky * a ?.

   - Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
   - Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složce s názvem `Složka` a jejích podložkách. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.
   - Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.
6. Chcete-li z kontroly vyloučit určitý typ objektu, zadejte do pole **Objekt** název typu objektu podle klasifikace encyklopedie Kaspersky (například `Email-Worm`, `Rootkit` nebo `RemoteAdmin`).

   Můžete použít masky se znakem `?` (nahradí libovolný jeden znak) a znakem `*` (nahradí libovolný počet znaků). Je-li například zadána maska `Client*`, aplikace Kaspersky Endpoint Security vyloučí z kontroly objekty `Client-IRC`, `Client-P2P` a `Client-SMTP`.
7. Chcete-li z kontroly vyloučit jednotlivý soubor, do pole **Hodnota hash souboru** zadejte hodnotu hash tohoto souboru.

   V případě změny soubory se změní také hodnota hash souboru. V tomto případě nebude upravený soubor přidán k výjimkám.
8. V bloku **Součásti ochrany** vyberte součásti, pro které chcete výjimky z kontroly použít.
9. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.
10. Vyberte pro výjimku stav **Aktivní**.

    Pomocí přepínače můžete výjimku kdykoli ukončit.
11. Uložte změny.

Příklady masky cesty:
Cesty k souborům umístěným v libovolné složce:

- Maska `*.exe` bude reprezentovat všechny cesty k souborům, které mají příponu EXE.

- Maska `example*` bude představovat všechny cesty k souborům s názvem EXAMPLE.

Cesty k souborům umístěným v zadané složce:

- Maska `C:\dir\*.*` bude představovat všechny cesty k souborům umístěným ve složce C:\dir\, nikoli však v podsložkách složky C:\dir\.
- Maska `C:\dir\*` bude představovat všechny cesty k souborům umístěným ve složce C:\dir\, nikoli však v podsložkách složky C:\dir\.
- Maska `C:\dir\` bude představovat všechny cesty k souborům umístěným ve složce C:\dir\, nikoli však v podsložkách složky C:\dir\.
- Maska `C:\dir\*.exe` bude představovat všechny cesty k souborům s příponou EXE umístěným ve složce C:\dir\, nikoli však v podsložkách složky C:\dir\.
- Maska `C:\dir\test` bude představovat všechny cesty k souborům s názvem „test“ umístěným ve složce C:\dir\, nikoli však v podsložkách složky C:\dir\.
- Maska `C:\dir\*\test` bude představovat všechny cesty k souborům s názvem „test“ umístěným ve složce C:\dir\ a v podsložkách složky C:\dir\.

Cesty k souborům umístěným ve všech složkách se zadaným názvem:

- Maska `dir\*.*` bude představovat všechny cesty k souborům ve složkách s názvem „dir“, nikoli však v podsložkách těchto složek.
- Maska `dir\*` bude představovat všechny cesty k souborům ve složkách s názvem „dir“, nikoli však v podsložkách těchto složek.
- Maska `dir\` bude představovat všechny cesty k souborům ve složkách s názvem „dir“, nikoli však v podsložkách těchto složek.
- Maska `dir\*.exe` bude představovat všechny cesty k souborům s příponou EXE ve složkách s názvem „dir“, nikoli však v podsložkách těchto složek.
- Maska `dir\test` bude představovat všechny cesty k souborům s názvem „test“ ve složkách s názvem „dir“, nikoli však v podsložkách těchto složek.

Povolení a zakázání výjimky z kontroly

Postup povolení nebo zakázání výjimky z kontroly:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.
4. Vyberte požadovanou výjimku ze seznamu výjimek z kontroly.
5. Pomocí přepínače vedle objektu můžete tento objekt zahrnout do rozsahu kontroly nebo jej vyloučit.

6. Uložte změny.

Úprava seznamu důvěryhodných aplikací

Seznam důvěryhodných aplikací je seznam aplikací, jejichž činnost se soubory a v síti (včetně škodlivé činnost) a přístup k systémovému registru nejsou aplikací Kaspersky Endpoint Security sledovány. Aplikace Kaspersky Endpoint Security ve výchozím nastavení kontroluje objekty, které jsou otevírané, spouštěné nebo ukládané jakýmkoli procesem aplikace, a kontroluje činnost všech aplikací a veškerý síťový provoz, který tyto aplikace vygenerují. Aplikace, která byla přidána do seznamu důvěryhodných aplikací, je však z kontroly aplikací Kaspersky Endpoint Security vyloučena.

Pokud například považujete objekty používané standardní aplikací Poznámkový blok v systému Microsoft Windows za bezpečnou, takže ji není třeba kontrolovat (tj. této aplikaci důvěřujete), může ji přidat na seznam důvěryhodných aplikací. Při kontrole jsou pak vynechány objekty, které tato aplikace používá.

Kromě toho mohou být některé akce, které jsou klasifikované aplikací Kaspersky Endpoint Security jako podezřelé, v kontextu funkcí řady aplikací bezpečné. Například zachycení textu psaného na klávesnici je běžný proces pro automatické přepínače rozvržení klávesnice (například Punto Switcher). Pokud chcete zohlednit specifika takových aplikací a vyloučit jejich činnost ze sledování, doporučujeme je přidat na seznam důvěryhodných aplikací.

Vyloučení důvěryhodných aplikací z kontrol umožňuje zabránit konfliktům kompatibility mezi aplikací Kaspersky Endpoint Security a jinými programy (například problém zdvojené kontroly síťového provozu počítače třetí strany pomocí aplikace Kaspersky Endpoint Security a jiné antivirové aplikace) a také zvyšuje výkon počítače, což je důležité při použití serverových aplikací.

U důvěryhodných aplikací jsou i nadále příslušné spustitelné soubory a procesy kontrolovány na viry či jiný malware. Za použití výjimek z kontroly lze aplikaci plně vyloučit z kontrol prováděných aplikací Kaspersky Endpoint Security.

Jak přidat aplikaci na seznam důvěryhodných v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnosti **Obecná nastavení** → **Výjimky**.
6. V části **Výjimky z kontroly a důvěryhodné aplikace** klikněte na tlačítko **Nastavení**.
7. V okně **Důvěryhodná zóna** vyberte kartu **Důvěryhodné aplikace**.

   Otevře se okno obsahující seznam důvěryhodných aplikací.
8. Pokud chcete vytvořit konsolidovaný seznam důvěryhodných aplikací pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy důvěryhodných aplikací v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Důvěryhodné aplikace z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna nebo odstranění důvěryhodných aplikací v nadřazené zásadě nejsou možné.
9. Pokud chcete uživateli umožnit vytvoření místního seznamu důvěryhodných aplikací, zaškrtněte políčko **Povolit používání místních důvěryhodných aplikací**. Tímto způsobem může uživatel kromě obecného seznamu důvěryhodných aplikací generovaného v zásadách vytvořit svůj vlastní místní seznam důvěryhodných aplikací. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu důvěryhodných aplikací generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené důvěryhodné aplikace z kontroly.
10. Klikněte na tlačítko **Přidat**.
11. V okně, které se otevře, zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

    Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

    > Kaspersky Endpoint Security nepodporuje při generování seznamu důvěryhodných aplikací v konzole aplikace Kaspersky Security Center proměnnou prostředí `%userprofile%`. Chcete-li položku použít na všechny uživatelské účty, můžete použít znak * (například `C:\Users\*\Documents\File.exe`).

    > Kdykoli přidáte novou proměnnou prostředí, musíte restartovat aplikaci.
12. Nakonfigurujte rozšířené nastavení pro důvěryhodnou aplikaci (viz tabulka níže).
13. Pomocí zaškrtávacího políčka můžete aplikaci z důvěryhodné zóny kdykoli vyloučit.
14. Uložte změny.

[Jak přidat aplikaci na seznam důvěryhodných aplikací ve webové konzole a cloudové konzole](#)

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete přidat aplikaci na seznam důvěryhodných aplikací.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte položky **Obecná nastavení** → **Výjimky**.
5. V bloku **Výjimky z kontroly a důvěryhodné aplikace** klikněte na odkaz **Důvěryhodné aplikace**.

   Otevře se okno obsahující seznam důvěryhodných aplikací.
6. Pokud chcete vytvořit konsolidovaný seznam důvěryhodných aplikací pro všechny počítače ve společnosti, zaškrtněte políčko **Sloučit hodnoty při dědění**. Seznamy důvěryhodných aplikací v nadřazené a podřízené zásadě budou sloučeny. Seznamy budou sloučeny za předpokladu, že je povoleno slučování hodnot při dědění. Důvěryhodné aplikace z nadřazené zásady se zobrazují v podřízených zásadách v zobrazení jen pro čtení. Změna nebo odstranění důvěryhodných aplikací v nadřazené zásadě nejsou možné.
7. Pokud chcete uživateli umožnit vytvoření místního seznamu důvěryhodných aplikací, zaškrtněte políčko **Povolit používání místních důvěryhodných aplikací**. Tímto způsobem může uživatel kromě obecného seznamu důvěryhodných aplikací generovaného v zásadách vytvořit svůj vlastní místní seznam důvěryhodných aplikací. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače.

   Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu důvěryhodných aplikací generovanému v zásadách. Pokud byl vygenerován místní seznam, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené důvěryhodné aplikace z kontroly.
8. Klikněte na tlačítko **Přidat**.
9. V okně, které se otevře, zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

   Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

   > Kaspersky Endpoint Security nepodporuje při generování seznamu důvěryhodných aplikací v konzole aplikace Kaspersky Security Center proměnnou prostředí `%userprofile%`. Chcete-li položku použít na všechny uživatelské účty, můžete použít znak * (například `C:\Users\*\Documents\File.exe`).

   > Kdykoli přidáte novou proměnnou prostředí, musíte restartovat aplikaci.
10. Nakonfigurujte rozšířené nastavení pro důvěryhodnou aplikaci (viz tabulka níže).
11. Pomocí zaškrtávacího políčka můžete aplikaci z důvěryhodné zóny kdykoli vyloučit.
12. Uložte změny.

[Jak přidat aplikaci na seznam důvěryhodných v rozhraní aplikace](#)

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.
4. V daném okně klikněte na tlačítko **Přidat**.
5. Vyberte spustitelný soubor důvěryhodné aplikace.

   Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

   Aplikace Kaspersky Endpoint Security podporuje proměnné prostředí a převádí cestu v místním rozhraní aplikace. Jinými slovy, pokud zadáte cestu k souboru `%userprofile%\Documents\File.exe`, do místního rozhraní aplikace pro uživatele Fred123 se přidá záznam `C:\Users\Fred123\Documents\File.exe`. Kaspersky Endpoint Security tak bude ignorovat důvěryhodný program `File.exe` u jiných uživatelů. Chcete-li položku použít na účty všech uživatelů, můžete použít znak `*` (například `C:\Users\*\Documents\File.exe`).

   Kdykoli přidáte novou proměnnou prostředí, musíte restartovat aplikaci.
6. V okně vlastností důvěryhodné aplikace nakonfigurujte rozšířené nastavení (viz tabulka níže).
7. Pomocí přepínače můžete aplikaci z důvěryhodné zóny kdykoli vyloučit.
8. Uložte změny.

Nastavení důvěryhodné aplikace

Parametr	Popis
Nekontrolovat otevírané soubory	Z kontroly aplikací Kaspersky Endpoint Security jsou vyloučeny všechny soubory, které otevírá tato aplikace. Pokud například používáte aplikace k zálohování souborů, tato funkce pomáhá snížit spotřebu prostředků aplikací Kaspersky Endpoint Security.
Nesledovat činnost aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat souborovou ani síťovou aktivitu aplikace v operačním systému. Činnost aplikace je monitorována následujícími součástmi: Detekce chování, Prevence zneužití, Prevence narušení hostitele, Nástroj pro nápravu a Brána firewall.
Nedědit omezení nadřazeného procesu (aplikace)	Omezení nakonfigurovaná pro nadřazený proces nebude aplikace Kaspersky Endpoint Security používat na podřízený proces. Nadřazený proces je spuštěn aplikací, pro kterou jsou nakonfigurována práva aplikace (Prevence narušení hostitele) a pravidla sítě aplikace (Brána firewall).
Nesledovat činnost podřízených aplikací	Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu souborů ani síťovou aktivitu aplikací spuštěných touto aplikací.
Povolit interakci s rozhraním aplikace Kaspersky	Sebeobrana aplikace Kaspersky Endpoint Security blokuje všechny pokusy o správu služeb aplikace ze vzdáleného počítače. Je-li políčko vybráno, je aplikaci se vzdáleným přístupem povoleno spravovat nastavení aplikace Kaspersky Endpoint Security prostřednictvím rozhraní aplikace Kaspersky Endpoint Security.

Endpoint Security	
Neblokovat interakci se součástí Ochrana AMSI *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Aplikace Kaspersky Endpoint Security nebude monitorovat požadavky důvěryhodné aplikace na objekty, které mají být kontrolovány součástí Ochrana AMSI.
Nekontrolovat šifrovaný provoz / Nekontrolovat veškerý provoz	Síťový provoz iniciovaný touto aplikací bude vyloučen z kontroly aplikací Kaspersky Endpoint Security. Z kontroly můžete vyloučit buď veškerý provoz, nebo pouze šifrovaný provoz. Z kontroly můžete také vyloučit jednotlivé adresy IP a čísla portů.
Poznámka	V případě potřeby můžete uvést krátký komentář k důvěryhodné aplikaci. Komentáře pomáhají zjednodušit vyhledávání a řazení důvěryhodných aplikací.
Stav	Stav důvěryhodné aplikace: • **Aktivní** stav znamená, že aplikace patří do důvěryhodné zóny. • **Neaktivní** stav znamená, že je aplikace vyloučena z důvěryhodné zóny.

Povolení a zakázání pravidel důvěryhodné zóny pro aplikaci v seznamu důvěryhodných aplikací

Postup povolení nebo zakázání akce pravidel důvěryhodné zóny použitých na aplikaci ze seznamu důvěryhodných aplikací:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.
4. V seznamu důvěryhodných aplikací vyberte požadovanou důvěryhodnou aplikaci.
5. Pomocí přepínače ve sloupci **Stav** můžete tento objekt zahrnout do rozsahu kontroly nebo jej vyloučit.
6. Uložte změny.

Použití důvěryhodného úložiště certifikátů systému

Použití úložiště certifikátů systému umožňuje vyjmout aplikace s důvěryhodným digitálním podpisem z antivirových kontrol. Kaspersky Endpoint Security automaticky přiřadí takové aplikace do skupiny *Důvěryhodné*.

Postup pro použití důvěryhodného úložiště certifikátů systému:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V rozevíracím seznamu **Úložiště důvěryhodných systémových certifikátů** vyberte, které systémové úložiště má aplikace Kaspersky Endpoint Security považovat za důvěryhodné.
4. Uložte změny.

Správa zálohy

Funkce *zálohování* ukládá záložní kopie souborů, které byly odstraněny nebo změněny během dezinfekce. *Záložní kopie* je kopie souboru vytvořená, předtím než byl soubor dezinfikován nebo odstraněn. Záložní kopie souborů jsou ukládány ve zvláštním formátu a nepředstavují hrozbu.

Záložní kopie souborů jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES\QB`.

Uživatelům ve skupině správců je uděleno úplné oprávnění pro přístup k této složce. Uživateli, jehož účet byl použit k instalaci aplikace Kaspersky Endpoint Security, jsou udělena omezená přístupová práva k této složce.

Aplikace Kaspersky Endpoint Security neposkytuje možnost konfigurace přístupových oprávnění uživatele za účelem zálohování kopií souborů.

Někdy se stane, že během dezinfekce nelze zachovat integritu souborů. Pokud přijdete částečně nebo zcela o přístup k důležitým informacím v dezinfikovaném souboru, můžete se pokusit obnovit soubor ze záložní kopie v původní složce.

Pokud je aplikace Kaspersky Endpoint Security spuštěna pod správou aplikace Kaspersky Security Center, záložní kopie souborů mohou být přeneseny na administrační server Kaspersky Security Center. Podrobnější informace o správě záložních kopií souborů v aplikaci Kaspersky Security Center najdete v systému nápovědy k aplikaci Kaspersky Security Center.

Konfigurace maximální doby uložení souborů v záloze

Výchozí maximální doba uložení kopií souborů v záloze je 30 dní. Po uplynutí maximální doby uložení aplikace Kaspersky Endpoint Security nejstarší soubory ze složky záloh odstraní.

Postup konfigurace maximální doby uložení souborů v záloze:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Zprávy a úložiště**.
3. Chcete-li omezit dobu uložení kopií souborů v záloze, zaškrtněte políčko **Neukládat objekty déle než N dní** v bloku **Záloha**. Do pole vpravo od zaškrtávacího políčka **Neukládat objekty déle než N dní** zadejte maximální dobu uložení kopií souborů v záloze.
4. Uložte změny.

Konfigurace maximální velikosti zálohy

Můžete určit maximální velikost zálohy. Velikost zálohy je ve výchozím nastavení neomezená. Po dosažení maximální velikosti aplikace Kaspersky Endpoint Security automaticky odstraní ze zálohy nejstarší soubory, aby maximální velikost nebyla překročena.

Postup konfigurace maximální velikosti zálohy:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně s nastavením aplikace vyberte část **Zprávy a úložiště**.

3. Pokud chcete omezit velikost zálohy, zaškrtněte políčko **Omezit velikost zálohy na N MB** v bloku **Záloha**. Zadejte maximální velikost zálohy.

4. Uložte změny.

Obnovení souborů ze zálohy

Pokud je v souboru zjištěn škodlivý kód, aplikace Kaspersky Endpoint Security tento soubor zablokuje, přiřadí mu stav *Infikovaný* a umístí jeho kopii do zálohy a pokusí se jej dezinfikovat. Pokud dezinfekce souboru proběhne úspěšně, stav záložní kopie souboru se změní na *Dezinfikováno*. Soubor bude k dispozici v původní složce. Pokud soubor nelze dezinfikovat, aplikace Kaspersky Endpoint Security jej odstraní z původní složky. Soubor záložní kopie můžete obnovit v původní složce.

Soubory se stavem *Při restartu počítače bude dezinfikováno* nelze obnovit. Restartujte počítač a stav souboru se změní na *Dezinfikováno* nebo *Smazáno*. Soubor záložní kopie můžete také obnovit v původní složce.

Když je zjištěn škodlivý kód v souboru, který je součástí aplikace ze služby Windows Store, aplikace Kaspersky Endpoint Security tento soubor okamžitě odstraní a jeho kopie není vložena do zálohy. Integritu aplikace ze služby Windows Store můžete obnovit pomocí příslušných nástrojů operačního systému Microsoft Windows 8 (podrobnosti o obnovení aplikace ze služby Windows Store najdete v *souborech nápovědy k systému Microsoft Windows 8*).

Sada záložních kopií souborů je nabízena jako tabulka. V případě záložní kopie souboru se zobrazí cesta k původní složce souboru. Cesta k původní složce souboru může obsahovat osobní data.

Pokud je do zálohy přesunuto několik souborů s identickými názvy a různým obsahem umístěných ve stejné složce, lze obnovit pouze poslední soubor umístěný do zálohy.

Postup obnovení souborů ze zálohy:

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Úložiště**.

   Otevře se okno **Záloha**.

2. V tabulce v okně **Záloha** vyberte jeden nebo více souborů v záloze.

3. Klikněte na tlačítko **Obnovit**.

   Aplikace Kaspersky Endpoint Security obnoví z vybraných záložních kopií soubory v původních složkách.

Odstranění záložních kopií souborů ze zálohy

Aplikace Kaspersky Endpoint Security automaticky odstraní ze zálohy záložní kopie souborů v jakémkoli stavu, jakmile uplyne doba jejich uložení, která je nakonfigurovaná v nastavení aplikace. Můžete také ručně odstranit libovolnou kopii souboru ze zálohy.

Postup odstranění záložních kopií souborů ze zálohy:

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Úložiště**.

   Otevře se okno **Záloha**.

2. Vyberte záložní kopie souborů, které chcete odstranit ze zálohy, a klikněte na tlačítko **Odstranit**. Můžete také odstranit všechny soubory ze zálohy kliknutím na tlačítko **Odstranit vše**.

Aplikace Kaspersky Endpoint Security odstraní ze zálohy vybrané záložní kopie souborů.

Oznamovací služba

Během provozu aplikace Kaspersky Endpoint Security dochází k celé řadě událostí. Upozornění na tyto události může být čistě informační nebo může obsahovat kritické informace. Upozornění mohou například informovat o úspěšné aktualizaci databází a modulů aplikace nebo do protokolu zaznamenat chyby součástí, které je třeba opravit.

Aplikace Kaspersky Endpoint Security podporuje protokolování informací o událostech v provozu do aplikačního protokolu systému Microsoft Windows nebo protokolu událostí aplikace Kaspersky Endpoint Security.

Aplikace Kaspersky Endpoint Security poskytuje upozornění následujícími způsoby:

- pomocí místních oznámení v oznamovací oblasti hlavního panelu systému Microsoft Windows;
- pomocí e-mailu.

Doručování upozornění na události můžete konfigurovat. Způsob doručování upozornění je nakonfigurován pro každý typ události.

Při použití tabulky událostí ke konfiguraci oznamovací služby můžete provést následující akce:

- filtrování událostí oznamovací služby podle hodnot sloupce nebo vlastních podmínek filtru;
- použití funkce hledání k hledání událostí oznamovací služby;
- řazení událostí oznamovací služby;
- změna pořadí a nastavení sloupců, které se zobrazují v seznamu událostí oznamovací služby.

Konfigurace nastavení protokolů událostí

Postup konfigurace nastavení protokolů událostí:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně s nastavením aplikace vyberte část **Rozhraní**.
3. V části **Upozornění** klikněte na tlačítko **Nastavit upozornění**.

   Součásti a úlohy aplikace Kaspersky Endpoint Security jsou uvedeny v levé části okna. Pravá část okna uvádí seznam událostí, k nimž došlo v souvislosti s vybranou součástí nebo úlohou.

   Události mohou obsahovat následující uživatelská data:

   - cesty k souborům kontrolovaným aplikací Kaspersky Endpoint Security;
   - cesty ke klíčům registru upraveným během činnosti aplikace Kaspersky Endpoint Security;
   - jméno uživatele systému Microsoft Windows;
   - adresy webových stránek otevřených uživatelem.
4. V levé části okna vyberte součást nebo úlohu, pro kterou chcete konfigurovat nastavení protokolu událostí.

5. Zaškrtněte políčka u odpovídajících událostí ve sloupcích **Uložit do místní zprávy** a **Uložit do protokolu událostí systému Windows**.

   Události, jejichž políčka jsou zaškrtnuta ve sloupci **Uložit do místní zprávy**, se zobrazují v seznamu **Protokoly aplikací a služeb** v části **Protokol událostí Kaspersky**. Události, jejichž políčka jsou zaškrtnuta ve sloupci **Uložit do protokolu událostí systému Windows**, jsou zobrazeny v seznamu **Protokoly systému Windows** v části **Aplikace**. Chcete-li otevřít protokoly událostí, vyberte položky **Start → Ovládací panely → Správa → Prohlížeč událostí**.

6. Uložte změny.

Konfigurace zobrazení a doručování upozornění

Postup konfigurace zobrazení a doručování upozornění:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně s nastavením aplikace vyberte část **Rozhraní**.

3. V části **Upozornění** klikněte na tlačítko **Nastavit upozornění**.

   Součásti a úlohy aplikace Kaspersky Endpoint Security jsou uvedeny v levé části okna. Pravá část okna uvádí seznam událostí, k nimž došlo v souvislosti s vybranou úlohou.

   Události mohou obsahovat následující uživatelská data:

   - cesty k souborům kontrolovaným aplikací Kaspersky Endpoint Security;
   - cesty ke klíčům registru upraveným během činnosti aplikace Kaspersky Endpoint Security;
   - jméno uživatele systému Microsoft Windows;
   - adresy webových stránek otevřených uživatelem.

4. V levé části okna vyberte součást nebo úlohu, pro kterou chcete konfigurovat doručování upozornění.

5. Ve sloupci **Upozornit na obrazovce** zaškrtněte políčka vedle požadovaných událostí.

   Informace o vybraných událostech se zobrazí na obrazovce v podobě zpráv v oznamovací oblasti hlavního panelu systému Microsoft Windows.

6. Ve sloupci **Upozornit e-mailem** zaškrtněte políčka vedle požadovaných událostí.

   Informace o vybraných událostech budou doručovány e-mailem v případě, že je nakonfigurováno nastavení doručování.

7. Klikněte na tlačítko **OK**.

8. Pokud jste povolili e-mailová upozornění, nakonfigurujte nastavení pro doručování e-mailů:

   a. Klikněte na tlačítko **Nastavení upozornění elektronickou poštou**.

   b. Zaškrtnutím políčka **Upozorňovat na události** povolíte doručování informací o událostech aplikace Kaspersky Endpoint Security vybraných ve sloupci **Upozornit e-mailem**.

   c. Určete nastavení doručování upozornění elektronickou poštou.

d. Klikněte na tlačítko **OK**.

9. Uložte změny.

Konfigurace zobrazení varování v oznamovací oblasti, která se týkají stavu aplikace

Postup konfigurace zobrazení varování v oznamovací oblasti, která se týkají stavu aplikace:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně s nastavením aplikace vyberte část **Rozhraní**.

3. V části **Zobrazovat stav aplikace v oznamovací oblasti** zaškrtněte políčka vedle kategorií událostí, o nichž chcete zobrazovat upozornění v oznamovací oblasti systému Microsoft Windows.

4. Uložte změny.

Když nastanou události související s vybranými kategoriemi, ikona aplikace v oznamovací oblasti se změní na nebo v závislosti na závažnosti varování.

Správa zpráv

Ve zprávách jsou zaznamenávány informace o provozu každé součásti aplikace Kaspersky Endpoint Security, událostech šifrování dat, provedení každé úlohy kontroly, úlohy aktualizace, úlohy kontroly integrity a také o celkovém fungování aplikace.

Zprávy jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES\Report`.

Zprávy mohou obsahovat následující uživatelská data:

- cesty k souborům kontrolovaným aplikací Kaspersky Endpoint Security;
- cesty ke klíčům registru upraveným během činnosti aplikace Kaspersky Endpoint Security;
- jméno uživatele systému Microsoft Windows;
- adresy webových stránek otevřených uživatelem.

Údaje ve zprávě jsou uvedeny v tabulkové formě. Každý řádek tabulky obsahuje informace o jedné události. Ve sloupcích tabulky jsou atributy události. Některé sloupce jsou složené a obsahují vnořené sloupce s dalšími atributy. Chcete-li zobrazit další atributy, klikněte na tlačítko ⊞ vedle názvu sloupce. Události, které jsou zaznamenávány během provozu různých součástí nebo provádění různách úloh, mají různé sady atributů.

K dispozici jsou následující zprávy:

- Zpráva **Audit systému**. Obsahuje informace o událostech, k nimž došlo během interakce uživatele s aplikací a při obecném provozu aplikace. Jsou to události, které nesouvisí s žádnou konkrétní součástí nebo úlohou aplikace Kaspersky Endpoint Security.
- Zprávy o provozu součástí aplikace Kaspersky Endpoint Security.
- Zprávy o úlohách aplikace Kaspersky Endpoint Security.
- Zpráva **Šifrování dat**. Obsahuje informace o událostech, k nimž došlo během šifrování a dešifrování dat.

Ve zprávách se používají následující úrovně důležitosti události:

Informační zprávy. Referenční události, které obvykle neobsahují důležité informace.

Varování. Události vyžadující pozornost, jelikož se týkají důležitých situací v rámci provozu aplikace Kaspersky Endpoint Security.

Kritické události. Události kritické důležitosti, které označují problémy s provozem aplikace Kaspersky Endpoint Security nebo zranitelnosti zjištěné v počítači uživatele.

Chcete-li zjednodušit zpracování zpráv, můžete data nabízená na obrazovce upravit následujícími způsoby:

- filtrování seznamu událostí podle různých kritérií;
- použití funkce hledání k vyhledání určité události;
- zobrazení vybrané události v samostatné části;
- řazení seznamu událostí podle jednotlivých sloupců zprávy;

- zobrazení a skrytí událostí seskupených podle filtru událostí pomocí tlačítka ⊞;
- změna pořadí a uspořádání sloupců, které se ve zprávě zobrazují.

Vygenerovanou zprávu můžete v případě potřeby uložit do textového souboru. Také můžete odstranit informace zpráv o součástech a úlohách aplikace Kaspersky Endpoint Security, které jsou sloučené do skupin.

Pokud je aplikace Kaspersky Endpoint Security spuštěna pod správou aplikace Kaspersky Security Center, mohou být informace o událostech předávány na server pro správu Kaspersky Security Center (další podrobnosti naleznete v *průvodci nápovědou k aplikaci Kaspersky Security Center*).

Zobrazení sestav

Pokud uživatel může zobrazit zprávy, může zobrazit také všechny události zahrnuté ve zprávě.

Postup zobrazení zpráv:

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Zprávy**.
2. V levé části okna **Zprávy** vyberte v seznamu součástí a úloh požadovanou součást nebo úlohu.

   V pravé části okna se zobrazí zpráva obsahující seznam událostí vyplývajících z činnosti vybrané součásti nebo vybrané úlohy aplikace Kaspersky Endpoint Security. Události ve zprávě můžete seřadit na základě hodnot v buňkách některého ze sloupců. Události zpráv jsou ve výchozím nastavení řazeny vzestupně podle hodnot v buňkách ve sloupci **Datum události**.
3. Chcete-li zobrazit podrobné informace o události, vyberte událost ve zprávě.

   V dolní části okna se zobrazí část se shrnutím události.

Konfigurace maximální doby uchovávání zpráv

Výchozí maximální doba uchovávání zpráv o událostech protokolovaných aplikací Kaspersky Endpoint Security je 30 dní. Po této době bude aplikace Kaspersky Endpoint Security automaticky mazat nejstarší záznamy ze souboru zprávy.

Postup změny maximální doby uchovávání zpráv:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Zprávy a úložiště**.
3. Chcete-li omezit dobu uložení zprávy, zaškrtněte v bloku **Zprávy** zaškrtávací políčko **Neukládat zprávy déle než N dní**. Určete maximální dobu uchovávání zpráv.
4. Uložte změny.

Konfigurace maximální velikosti souboru zprávy

Můžete nastavit maximální velikost souboru obsahujícího zprávu. Ve výchozím nastavení je maximální velikost souboru zprávy 1024 MB. Aby nedošlo k překročení maximální velikosti souboru zprávy, bude aplikace Kaspersky Endpoint Security po dosažení maximální velikosti automaticky mazat nejstarší záznamy.

Postup konfigurace maximální velikosti souboru zprávy:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Zprávy a úložiště**.
3. Pokud chcete omezit velikost souboru sestavy, v bloku **Zprávy** zaškrtněte políčko **Omezit velikost souboru sestavy na N MB**. Určete maximální velikost souboru zprávy.
4. Uložte změny.

Uložení zprávy do souboru

Uživatel je osobně odpovědný za zabezpečení informací ze zprávy uložených do souboru, a především za kontrolu těchto informací a omezení přístupu k nim.

Vygenerované zprávy můžete uložit do souboru v textovém formátu TXT nebo ve formátu CSV.

Aplikace Kaspersky Endpoint Security zaznamenává události do zpráv stejným způsobem, jakým se zobrazují na obrazovce. To znamená, že za použití stejné sady a sekvence atributů události.

Postup uložení zprávy do souboru:

1. V hlavním okně aplikace klikněte na **Další nástroje** → **Zprávy**.
2. V okně, které se otevře, vyberte součást nebo úlohu.

   V pravé části okna se zobrazí zpráva, která obsahuje seznam událostí, k nimž došlo během provozu vybrané součásti nebo v průběhu prováděné úlohy aplikace Kaspersky Endpoint Security.
3. V případě potřeby můžete nabízená data ve zprávě upravit následujícími akcemi:
   - filtrování událostí;
   - vyhledání události;
   - změna uspořádání sloupců;
   - řazení událostí.
4. V horní pravé části okna klikněte na tlačítko **Uložit zprávu**.
5. V okně, které se otevře, zadejte pro soubor zprávy cílovou složku.
6. Do pole **Název souboru** zadejte název souboru zprávy.
7. V poli **Typ souboru** vyberte požadovaný formát souboru zprávy: TXT nebo CSV.

8. Uložte změny.

Mazání zpráv

Postup odebrání informací ze zpráv:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně s nastavením aplikace vyberte část **Zprávy a úložiště**.
3. V bloku **Zprávy** klikněte na tlačítko **Vymazat**.
4. Pokud je povolena ochrana heslem, aplikace Kaspersky Endpoint Security vás může vyzvat k zadání přihlašovacích údajů k uživatelskému účtu. Pokud uživatel nemá požadovaná oprávnění, aplikace vyzve k zadání přihlašovacích údajů k účtu.

Aplikace Kaspersky Endpoint Security odstraní všechny zprávy pro všechny součásti a úlohy aplikace.

Sebeobrana aplikace Kaspersky Endpoint Security

Aplikace Kaspersky Endpoint Security chrání počítač před škodlivými aplikacemi, které se pokoušejí o blokování provozu aplikace Kaspersky Endpoint Security, či dokonce její odstranění z počítače. Sada dostupných technologií sebeobrany pro aplikaci Kaspersky Endpoint Security závisí na tom, zda je systém 32bitový, nebo 64bitový (viz tabulka níže).

Technologie sebeobrany aplikace Kaspersky Endpoint Security

Technologie	Popis	Počítač x86	Počítač x64
Mechanismus sebeobrany	Tato technologie blokuje přístup k následujícím součástem aplikace: • Soubory v instalační složce aplikace Kaspersky Endpoint Security • Klíče registru se záznamy patřícími aplikaci • Procesy spuštěné aplikací	✓	✓
AM-PPL (Antimalware Protected Process Light)	Tato technologie chrání procesy aplikace Kaspersky Endpoint Security před škodlivými akcemi. Podrobnější informace o fungování technologie AM-PPL najdete na webu společnosti Microsoft. Technologie AM-PPL je k dispozici pro operační systémy Windows 10 verze 1703 (RS2) nebo novější a pro operační systémy Windows Server 2019.	✓	–
Mechanismus obrany proti externí správě	Tato technologie omezuje správu aplikace Kaspersky Endpoint Security pomocí zvláštních aplikací pro vzdálenou správu (jako je TeamViewer nebo RemotelyAnywhere).	✓	– (kromě Windows 7)

Povolení a zakázání sebeobrany

Mechanismus sebeobrany aplikace Kaspersky Endpoint Security je ve výchozím nastavení povolen.

Postup povolení nebo zakázání sebeobrany:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Obecné**.
3. Pomocí zaškrtávacího políčka **Povolit sebeobranu** aktivujte nebo deaktivujte mechanismus sebeobrany.
4. Uložte změny.

Povolení a zakázání podpory technologie AM-PPL

Aplikace Kaspersky Endpoint Security podporuje technologii Antimalware Protected Process Light (dále jen „AM-PPL“) od společnosti Microsoft. AM-PPL chrání procesy aplikace Kaspersky Endpoint Security před škodlivými akcemi (například ukončením aplikace). AM-PPL umožňuje spouštět pouze důvěryhodné procesy. Procesy aplikace Kaspersky Endpoint Security jsou podepsány v souladu s bezpečnostními požadavky Windows, a proto jsou důvěryhodné. Podrobnější informace o fungování technologie AM-PPL najdete na webu společnosti Microsoft. Technologie AM-PPL je ve výchozím nastavení povolena.

Aplikace Kaspersky Endpoint Security má také vestavěné mechanismy pro ochranu procesů aplikace. Podpora AM-PPL umožňuje delegovat funkce zabezpečení procesů na operační systém. Můžete tak zvýšit rychlost aplikace a snížit spotřebu počítačových prostředků.

Služba AM-PPL je k dispozici pro operační systémy Windows 10 verze 1703 (RS2) nebo novější a pro operační systémy Windows Server 2019.

Postup povolení nebo zakázání technologie AM-PPL:

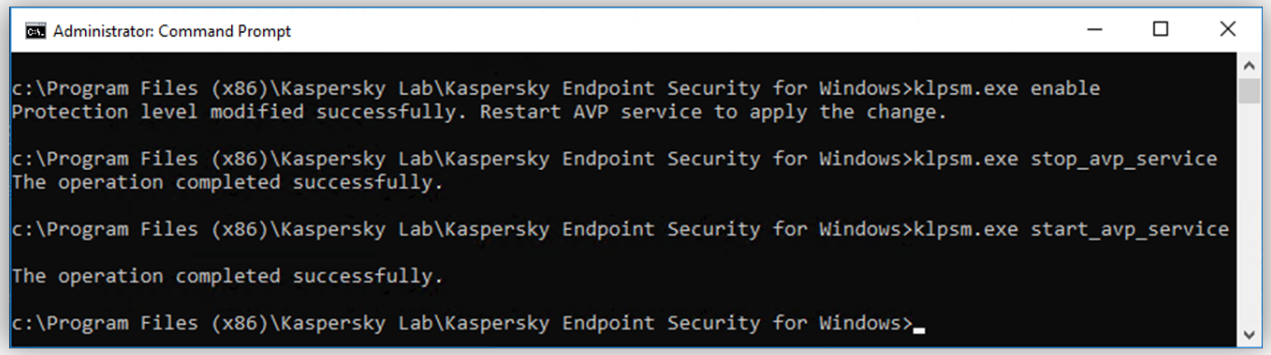
1. Vypněte mechanismus sebeobrany aplikace.

   Mechanismus sebeobrany zabraňuje úpravám a odstranění procesů aplikace v paměti počítače, včetně změny stavu služby AM-PPL.

2. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
3. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.
4. Do příkazového řádku zadejte následující:

   - `klpsm.exe enable` – povolí podporu technologie AM-PPL (viz obrázek níže).
   - `klpsm.exe disable` – zakáže podporu technologie AM-PPL.

5. Restartujte aplikaci Kaspersky Endpoint Security.
6. Obnoví mechanismus sebeobrany aplikace.



Povolení podpory technologie AM-PPL

Povolení a zakázání obrany proti externí správě

Ochrana proti externí správě vám umožňuje zakázat správu aplikace Kaspersky Endpoint Security pomocí aplikací pro vzdálenou správu (jako je TeamViewer nebo RemotelyAnywhere). Tato technologie slouží k následujícím účelům:

- Ochrana proti úpravě nastavení aplikace Kaspersky Endpoint Security.
- Ochrana proti správě služeb Kaspersky Endpoint Security (jako je služba `AVP`).
- Ochrana před zastavením procesů aplikace.

Ochrana před externí správou je k dispozici pouze pro počítače s 32bitovými operačními systémy. Tato technologie není k dispozici pro počítače se 64bitovými operačními systémy.

Postup povolení nebo zakázání ochrany proti externí správě:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená nastavení** → **Obecné**.
3. Zaškrtnutím políčka **Povolit správu nastavení aplikace Kaspersky Endpoint Security pomocí aplikací pro vzdálenou správu** povolíte nebo zakážete ochranu před úpravami nastavení aplikace Kaspersky Endpoint Security. Pokud používáte aplikace pro vzdálenou správu, měli byste povolit správu nastavení aplikace Kaspersky Endpoint Security a přidat aplikace do seznamu důvěryhodných. Nedůvěryhodné aplikace vzdálené správy nesmí upravovat nastavení aplikace Kaspersky Endpoint Security, ani když je zaškrtnuto políčko **Povolit správu nastavení aplikace Kaspersky Endpoint Security pomocí aplikací pro vzdálenou správu**. Toto zaškrtávací políčko není k dispozici, je-li zaškrtnuto políčko **Povolit sebeobranu**.
4. Pomocí zaškrtávacího políčka **Povolit vnější řízení služby** povolíte nebo zakažte ochranu služeb Kaspersky Endpoint Security před externí správou.

   Chcete-li aplikaci ukončovat z příkazového řádku, zakažte ochranu služeb Kaspersky Endpoint Security před externí správou.
5. Uložte změny.

Když jsou povoleny mechanismy obrany proti externí správě, aplikace Kaspersky Endpoint Security brání tomu, aby ukazatel myši směřoval na ikonu aplikace. Když se vzdálený uživatel pokusí službu aplikace vypnout, zobrazí se okno systému s chybovou zprávou.

Podpora aplikací vzdálené správy

Příležitostně může být nezbytné použít aplikaci pro vzdálenou správu, když je povolena obrana proti externímu správě.

Postup povolení provozu aplikací vzdálené správy:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.
4. V daném okně klikněte na tlačítko **Přidat**.
5. Vyberte spustitelný soubor aplikace pro vzdálenou správu.

Cestu můžete také zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

6. Zaškrtněte políčko **Nesledovat činnost aplikace**.

7. Uložte změny.

Výkon aplikace Kaspersky Endpoint Security a kompatibilita s jinými aplikacemi

Výkon aplikace Kaspersky Endpoint Security

Výkon aplikace Kaspersky Endpoint Security informuje o počtu typů zjistitelných objektů, které mohou být škodlivé pro počítač, a také o spotřebě energie a využití zdrojů počítače.

Výběr typů zjistitelných objektů

Aplikace Kaspersky Endpoint Security umožňuje detailně nastavit ochranu vašeho počítače a vybrat typy objektů, které bude během svého provozu detekovat. Aplikace Kaspersky Endpoint Security bude vždy kontrolovat přítomnost virů, červů a trojských koní v operačním systému. Kontrolu přítomnosti těchto typů objektů nelze zakázat. Malware tohoto typu může počítači způsobit závažné škody. Chcete-li zlepšit zabezpečení svého počítače, můžete rozšířit seznam typů zjistitelných objektů povolením monitorování legálního softwaru, který mohou využívat pachatelé k poškození počítače nebo osobních dat.

Použití režimu úspory energie

Množství energie spotřebované aplikacemi je pro přenosné počítače klíčovým faktorem. Naplánované úlohy aplikace Kaspersky Endpoint Security obvykle využívají výrazné množství systémových prostředků. Když je počítač napájen z baterií, můžete používat režim úspory energie, aby nebyla spotřeba energie příliš vysoká.

V režimu úspory energie jsou automaticky odloženy následující naplánované úlohy:

- úloha Aktualizace;
- úloha Úplná kontrola;
- úloha Kontrola kritických oblastí;
- úloha Vlastní kontrola;
- úloha Kontrola integrity.

Bez ohledu na to, zda je režim úspory energie povolen či nikoli, aplikace Kaspersky Endpoint Security pozastaví úlohy šifrování vždy, když přenosný počítač přejde na napájení z baterie. Úlohy šifrování pak aplikace obnoví, jakmile přenosný počítač znovu připojíte k napájení z elektrické sítě.

Uvolnění prostředků počítače pro jiné aplikace

Využití prostředků počítače aplikací Kaspersky Endpoint Security může mít dopad na výkon jiných aplikací. Aby nedocházelo k problémům se souběžnými operacemi při zvýšeném zatížení procesoru a pevného disku, dokáže aplikace Kaspersky Endpoint Security pozastavit naplánované úlohy a uvolnit prostředky pro jiné aplikace.

Nicméně řada aplikací se může spustit ihned po uvolnění prostředků procesoru a pokračovat v práci na pozadí. Aby nebyla kontrola závislá na výkonu jiných aplikací, je vhodnější jim prostředky operačního systému neuvolňovat.

Takovéto úlohy můžete v případě potřeby spustit ručně.

Použití technologie pokročilé dezinfekce

Moderní škodlivé aplikace mohou proniknout do nejhlubších úrovní operačního systému, takže je pak téměř nemožné je odstranit. Po zjištění škodlivé aktivity v operačním systému provede aplikace Kaspersky Endpoint Security rozsáhlý postup vyčištění, který využívá technologii pokročilé dezinfekce. *Technologie pokročilé dezinfekce* je zaměřena na očištění operačního systému od škodlivých aplikací, které již spustily své procesy v paměti RAM a které brání aplikaci Kaspersky Endpoint Security v odstranění jinými způsoby. Výsledkem je neutralizace hrozby. Zatímco probíhá pokročilá dezinfekce, neměli byste spouštět nové procesy ani upravovat registr operačního systému. Technologie pokročilé dezinfekce je velmi náročná na prostředky operačního systému, což může způsobit zpomalení chodu jiných aplikací.

Po dokončení postupu pokročilé dezinfekce v počítači s operačním systémem Microsoft Windows pro pracovní stanice si aplikace Kaspersky Endpoint Security od uživatele vyžádá svolení k restartování počítače. Po restartování systému aplikace Kaspersky Endpoint Security odstraní soubory malwaru a spustí úplnou kontrolu „lite“ celého počítače.

V počítačích se systémy Microsoft Windows pro servery není zobrazení žádosti o restartování možné kvůli vlastnostem aplikace Kaspersky Endpoint Security. Neplánované restartování souborového serveru může vést k problémům, jako je dočasná nedostupnost dat na serveru či ztráta neuložených dat. Souborové servery doporučujeme restartovat striktně v souladu s plánem. Z toho důvodu je technologie pokročilé dezinfekce u souborových serverů standardně zakázána.

V případě zjištění aktivní infekce v souborovém serveru dojde k předání události do aplikace Kaspersky Security Center s informací o tom, že je vyžadována aktivní dezinfekce. Pokud chcete odstranit aktivní infekci serveru, povolte technologii aktivní dezinfekce a spusťte skupinovou úlohu *antivirové kontroly* v době, která je vhodná pro uživatele serveru.

Výběr typů zjistitelných objektů

Postup výběru typů zjistitelných objektů:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V části **Typy zjišťovaných objektů** zaškrtněte políčka u typů objektů, které má aplikace Kaspersky Endpoint Security zjišťovat:
   - **Viry a červy**

Podkategorie: viry a červy (Viruses_and_Worms)

Úroveň hrozby: vysoká

Klasické viry a červy provádějí akce, které nejsou uživatelem schváleny. Mohou vytvářet kopie samy sebe, které se mohou replikovat.

Klasický virus

Když klasický virus pronikne do počítače, infikuje soubor, aktivuje se, provede škodlivé akce a přidá kopie sebe sama do jiných souborů.

Klasický virus se násobí pouze v místních prostředcích počítače, sám o sobě nemůže proniknout do jiných počítačů. Do jiného počítače může být přenesen, pouze pokud přidá kopii sebe sama do souboru, který je uložen ve sdílené složce nebo na vloženém disku CD, nebo pokud uživatel přepošle e-mailovou zprávu s připojeným infikovaným souborem.

Kód klasického viru může proniknout do různých oblastí počítačem operačních systémů a aplikací. V závislosti na prostředí se viry dělí na *souborové viry*, *spouštěcí viry*, *skriptové viry* a *makro viry*.

Viry mohou infikovat soubory různými technikami. *Přepisovací* viry přepíší svůj kód přes kód infikovaného souboru, čímž se obsah souboru vymaže. Infikovaný soubor přestane fungovat a nebude možné jej obnovit. *Parazitické* viry upravují soubory a zanechají se plně nebo částečně funkční. *Doprovodné viry* neupravují soubory, ale vytvářejí duplicitní soubory. Při otevření infikovaného souboru se spustí jeho duplikát (který je ve skutečnosti virem). Setkat se můžete také s následujícími typy virů: *odkazové viry*, *viry OBJ*, *viry LIB*, viry *zdrojového kódu* a mnoho dalších.

Červy

Stejně jako u klasického viru se po proniknutí do počítače aktivuje kód červa a provede škodlivé akce. Červy své označení získaly díky své schopnosti „plazit“ se z jednoho počítače do druhého a šířit kopie prostřednictvím různých datových kanálů bez povolení uživatele.

Hlavním prvkem, který umožňuje rozlišovat mezi různými typy červů, je způsob jejich šíření. Následující tabulka poskytuje přehled různých typů červů, které jsou klasifikovány dle způsobu šíření.

Způsob šíření červů

Typ	Název	Popis
Email-Worm	Email-Worm	Šíří se e-mailem. Infikovaná e-mailová zpráva obsahuje připojený soubor s kopií červa nebo odkaz na soubor nahraný na webovou stránku, která mohla být hacknuta nebo vytvořena speciálně pro tento účel. Když připojený soubor otevřete, červ se aktivuje. Když kliknete na odkaz, stáhnete a poté otevřete soubor, červ začne provádět škodlivé akce. Poté začne šířit své kopie, vyhledávat další e-mailové adresy a odesílat na ně infikované zprávy.
Červ IM	Klienti IM	Šíří se prostřednictvím klientů IM. Takové červy obvykle odesílají zprávy, které obsahují odkaz na soubor s kopií červa na webu, s využitím seznamů kontaktů uživatele. Když uživatel stáhne a otevře soubor, červ se aktivuje.
Červ IRC	Červi internetových konverzací	Šíří se prostřednictvím IRC (Internet Relay Chats), což jsou systémy služeb, které umožňují komunikaci s dalšími lidmi přes internet v reálném čase.

		Tyto červy zveřejní soubor s kopií jich samých nebo odkazem na soubor v internetové konverzaci. Když uživatel stáhne a otevře soubor, červ se aktivuje.
Síťový červ	Síťové červy	Tyto červy se šíří počítačovými sítěmi. Na rozdíl od jiných typů červů se běžný síťový červ šíří bez účasti uživatele. V místní síti hledá počítače, které obsahují zranitelné programy. Za tímto účelem odesílá speciálně vytvořený síťový paket (exploit), který obsahuje kód červa nebo jeho část. Pokud je v síti zranitelný počítač, obdrží takový síťový paket. Když červ zcela pronikne do počítače, aktivuje se.
Červ P2P	Síťové červy pro sdílení souborů	Šíří se přes sítě P2P pro sdílení souborů. Aby mohl červ infiltrovat síť P2P, zkopíruje se do složky pro sdílení souboru, která se obvykle nachází v počítači uživatele. V síti P2P se zobrazí informace o tomto souboru, aby uživatel mohl „najít“ infikovaný soubor v síti jako jakýkoli jiný soubor, stáhnout jej a otevřít. Propracovanější červy emulují síťový protokol určité sítě P2P: zobrazí kladné reakce na dotazy hledání a nabídnou kopie sebe sama ke stažení.
Červy	Další typy červů	Mezi další typy červů patří: • Červy, které šíří kopie sebe samých přes síťové prostředky. Pomocí funkcí operačního systémů prohledávají dostupné síťové složky, připojují se k počítačům na internetu a pokouší se získat plný přístup k diskovým jednotkám. Na rozdíl od dříve popsaných typů červů se jiné typy červů neaktivují samy, ale když uživatel otevře soubor, který obsahuje kopii červa. • Červi, kteří se šíří jinak než pomocí metod popsaných v předchozí tabulce (například červi šířící se mobilními telefony).

- Trojské koně

Podkategorie: Trojské koně

Úroveň hrozby: vysoká

Na rozdíl červů a virů se trojské koně samy nereplikují. Do počítače pronikají například přes e-mail nebo prohlížeč, když uživatel navštíví infikovanou webovou stránku. Trojské koně se spouští za účasti uživatele. Začínají provádět škodlivé akce ihned po spuštění.

Různé trojské koně se v infikovaných počítačích chovají různě. Mezi hlavní funkce trojských koňů patří blokování, úprava nebo ničení informací a zakázání počítačů nebo sítí. Trojské koně rovněž přijímají nebo odesílají soubory, spouští je, zobrazují zprávy na obrazovce, požadují webové stránky, stahují a instalují programy a restartují počítač.

Hackeři často používají sady trojských koňů.

Typy chování trojských koňů jsou popsány v následující tabulce.

Typy chování trojských koňů v infikovaném počítači

Typ	Název	Popis
Trojan-ArcBomb	Trojské koně – „archivní bomby“	Při rozbalení tyto archivy zvětší svou velikost do takové míry, že ovlivní činnost počítače. Když se uživatel pokusí takový archiv rozbalit, počítač se může zpomalit nebo zamrznout a pevný disk se může zaplnit „prázdnými“ daty. „Archivní bomby“ jsou nebezpečné především pro souborové a poštovní servery. Pokud server používá automatický systém zpracování příchozích informací, může „archivní bomba“ server zastavit.
Zadní vrátka	Trojské koně pro vzdálenou správu	Jsou považovány za nejnebezpečnější typ trojského koně. Z hlediska funkce se podobají aplikacím se vzdálenou správou, které jsou nainstalovány v počítači. Tyto programy se samy instalují do počítače, aniž by o tom uživatel věděl, takže útočník může počítač spravovat vzdáleně.
Trojský kůň	Trojské koně	Zahrnují následující škodlivé aplikace: • **Klasické trojské koně**. Tyto programy vykonávají pouze hlavní funkce trojských koňů: blokování, úpravu nebo ničení informací a zakazování počítačů nebo sítí. Nemají žádné pokročilé funkce, na rozdíl od trojských koňů popsaných v tabulce. • **Všestranné trojské koně**. Tyto programy mají rozšířené funkce typické pro několik typů trojských koňů.
Trojan-Ransom	Vyděračské trojské koně	Berou si údaje uživatele jako rukojmí, upravují je nebo blokují, nebo mají vliv na činnost počítače, takže uživatel ztratí možnost informace používat. Útočník požaduje od uživatele výkupné a slibuje zaslání aplikace pro obnovení výkonu počítače a dat, která v něm byla uložena.
Trojan-Clicker	Klikací trojské koně	Přistupují k webovým stránkám z počítače uživatele, odesláním příkazů do prohlížeče nebo změnou webových adres zadaných v souborech operačního systému. Použitím těchto programů útočníci páchají síťové útoky a zvyšují návštěvnost webů, čímž se zvyšuje počet zobrazení bannerových reklam.
Trojan-	Stahovací	Přecházejí na webovou stránku útočníka, stahují z ní další škodlivé

Downloader	trojské koně	aplikace a instalují je do počítače uživatele. Mohou obsahovat název souboru škodlivé aplikace, která bude stažena nebo získána z webové stránky, kterou otevíráte.
Trojan-Dropper	Přetahovací trojské koně	Obsahují další trojské koně, které instalují na pevný disk. Útočníci mohou programy typu Trojan Dropper používat k následujícím účelům: • Instalovat škodlivou aplikaci, aniž by si toho uživatel všiml: Programy typu Trojan Dropper nezobrazují žádné zprávy, nebo zobrazují falešné zprávy, které informují například o chybě v archivu nebo nekompatibilní verzi operačního systému. • Chránit jiné škodlivé aplikace před nalezením: ne každý antivirový software může zjistit škodlivou aplikaci v rámci aplikace typu Trojan Dropper.
Trojan-Notifier	Oznamovací trojské koně	Informují útočníka, že infikovaný počítač je přístupný, a odesílají útočníkovi informace o počítači: IP adresa, počet otevřených portů nebo e-mailová adresa. S útočníkem se spojují prostřednictvím e-mailu, serveru FTP, přístupu na webovou stránku útočníka nebo jinak. Programy typu Trojan Notifier se často používají v sadách tvořených několika trojskými koni. Informují útočníka, že byly do počítače uživatele úspěšně nainstalovány jiné trojské koně.
Trojan-Proxy	Trojské koně proxy	Umožňují útočníkům anonymní přístup k webovým stránkám pomocí počítače uživatele. Často se používají k odesílání nevyžádané pošty.
Trojan-PSW	Trojské koně pro krádeže hesel	Trojské koně pro krádeže hesel, které kradou uživatelské účty, jako například registrační údaje k softwaru. Tyto trojské koně hledají důvěrná data v systémových souborech a registrech a odesílají je „veliteli“ e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak. Některé z těchto trojských koňů jsou kategorizovány jako samostatné typy, které jsou popsány v této tabulce. Tyto trojské koně kradou bankovní účty (Trojan-Banker), kradou data od uživatelů klientů IM (Trojan-IM) a informace od hráčů online her (Trojan-GameThief).
Trojan-Spy	Špionské trojské koně	Špehují uživatele a shromažďují informace o akcích, které uživatel provede během práce na počítači. Mohou zachytit data, která uživatel zadává na klávesnici, pořizovat jejich snímky nebo shromažďovat seznamy aktivních aplikací. Po získání informací je předají útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak.
Trojan-DDoS	Trojské koně – síťoví útočníci	Odesílají různé požadavky z počítače uživatele na vzdálený server. Server postrádá prostředky na zpracování všech požadavků, takže přestane fungovat (Denial of Service neboli DoS – odmítnutí služby). Hackeři často infikují řadu počítačů těmito programy, aby mohli počítače uživatelů využít k současnému útoku na jeden server. Programy DoS útočí z jednoho počítače s vědomím uživatele. Programy DDoS (distribuované DoS) vykonávají distribuované útoky z několika počítačů, aniž by si toho uživatel infikovaného počítače všiml.
Trojan-IM	Trojské koně, které	Kradou čísla a hesla účtů uživatelů klientů posílání rychlých zpráv. Předávají data útočníkovi e-mailem, prostřednictvím serveru FTP,

	kradou informace od uživatelů klientů IM	přechodem na webovou stránku útočníka nebo jinak.
Rootkit	Rootkity	Maskují jiné škodlivé programy a jejich činnost, čímž prodlužují přítomnost aplikací v operačním systému. Rovněž ukrývají soubory, procesy v infikované paměti počítače nebo klíče registru, které spouští škodlivé aplikace. Rootkity mohou maskovat výměnu dat mezi aplikacemi v počítači uživatele a dalších počítačích v síti.
Trojan-SMS	Trojské koně v podobě zpráv SMS	Infikují mobilní telefony odesíláním zpráv SMS na telefonní čísla se sazbou za prémiové služby.
Trojan-GameThief	Trojské koně, které kradou informace od hráčů online her	Kradou přihlašovací údaje k účtům od hráčů online her a poté je odesílají útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak.
Trojan-Banker	Trojské koně, které kradou bankovní účty	Kradou údaje o bankovních účtech nebo data systémů elektronického bankovnictví a poté je odesílají hackerovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku hackera nebo jinou metodou.
Trojan-Mailfinder	Trojské koně, které shromažďují e-mailové adresy	Shromažďují e-mailové adresy, které ukládají do počítače, a odesílají je útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak. Útočníci mohou odesílat nevyžádanou poštu na adresy, které získali.

- Škodlivé nástroje

Podkategorie: Škodlivé nástroje

Úroveň nebezpečí: střední

Na rozdíl od jiných typů malwaru škodlivé nástroje neprovádějí své akce ihned po spuštění. Lze je v počítači uživatele bezpečně uložit a spustit. Útočníci často používají funkce těchto programů k vytváření virů, červů a trojských koňů, provádějí síťové útoky na vzdálených serverech, hackují počítače nebo provádějí jiné škodlivé akce.

Různé funkce škodlivých nástrojů jsou seskupeny dle typů popsaných v následující tabulce.

Funkce škodlivých nástrojů

Typ	Název	Popis
Konstruktor	Konstruktory	Umožňují vytváření nových virů, červů a trojských koňů. Některé konstruktory se chlubí standardním rozhraním se zobrazením v oknech, v nichž může uživatel vybrat typ škodlivé aplikace, který chce vytvořit, způsob boje s ladicími programy a další funkce.
Dos	Síťové útoky	Odesílají různé požadavky z počítače uživatele na vzdálený server. Server postrádá prostředky na zpracování všech požadavků, takže přestane fungovat (Denial of Service neboli DoS – odmítnutí služby).
Exploit	Exploity	Exploit je sada dat nebo programových kódů, která využívá zranitelnosti aplikace, ve které jsou zpracovány, a provádí v počítači škodlivou akci. Exploit může například zapisovat nebo číst soubory nebo požadovat infikované webové stránky. Různé exploity využívají zranitelnosti různých aplikací nebo síťových služeb. Exploit se tváří jako síťový paket a je přenášen sítí do několika počítačů, přičemž hledá počítače se zranitelnými síťovými službami. Exploit v souboru DOC využívá zranitelnosti textového editoru. Když uživatel otevře infikovaný soubor, může začít provádět akce, které jsou předprogramovány hackerem. Exploit vložený do e-mailové zprávy hledá zranitelnosti ve všech e-mailových klientech. Může začít provádět škodlivé akce, když uživatel otevře infikovanou zprávu v tomto e-mailovém klientovi. Červy Net-Worm se šíří v sítích pomocí exploitů. Nuker *exploity* jsou síťové pakety, které deaktivují počítače.
FileCryptor	Moduly pro šifrování	Šifrují jiné škodlivé aplikace a skrývají je před antivirovými aplikacemi.
Flooder	Programy pro kontaminaci sítí	Odesílají různé zprávy přes síťové kanály. Tento typ nástrojů zahrnuje například programy, které kontaminují systémy IRC (Internet Relay Chats). Nástroje typu Flooder nezahrnují programy, které kontaminují kanály používané e-mailem, klienty IM a systémy pro mobilní komunikaci. Tyto programy jsou samostatné typy popsané v tabulce (Email-Flooder, IM-Flooder a SMS-Flooder).
HackTool	Hackovací nástroje	Umožňují nabourat se do počítače, ve kterém jsou nainstalovány, nebo útočí na jiný počítač (například přidáním nových systémových účtů bez oprávnění uživatele nebo vymazáním protokolů systému za účelem zakrytí stop své přítomnosti v operačním systému). Tento typ nástrojů zahrnuje sledovací nástroje se škodlivými funkcemi, jako je například zachycení hesla. Sledovací programy umožňují zobrazení síťového provozu.

Hoax	Hoaxy	Varují uživatele zprávami o virech: mohou „zjistit virus“ v infikovaném souboru nebo informovat uživatele, že disk byl naformátován, ačkoli k tomu ve skutečnosti nedošlo.
Spoofer	Nástroje pro falšování adres	Odesílají zprávy a síťové požadavky s falešnou adresou odesilatele. Útočníci používají nástroje typu Spoofer například k tomu, aby byly považováni za skutečné odesilatele zpráv.
VirTool	Nástroje, které upravují škodlivé aplikace	Umožňují úpravu jiných malwarových programů, čímž je kryjí před antivirovými aplikacemi.
Email-Flooder	Programy, které kontaminují e-mailové adresy	Odesílají různé zprávy na různé e-mailové adresy, čímž je kontaminují. Velký objem příchozích zpráv brání uživatelům v zobrazení užitečných zpráv ve složce příchozích zpráv.
IM-Flooder	Programy, které kontaminují provoz klientů IM	Zaplavují uživatele klientů IM zprávami. Velký objem zpráv brání uživatelům v zobrazení užitečných příchozích zpráv.
SMS-Flooder	Programy, které kontaminují provoz zprávami SMS	Odesílají různé zprávy SMS na mobilní telefony.

- Adware

  Podkategorie: reklamní software (adware);

  Úroveň hrozby: střední

  Adware zobrazuje uživateli reklamní informace. Adwarové programy zobrazují bannerové reklamy v rozhraních jiných programů a přesměrovávají dotazy hledání na reklamní webové stránky. Některé z nich shromažďují marketingové informace o uživateli a odesílají je vývojáři: tyto informace mohou zahrnovat názvy webových stránek, které uživatel navštěvuje, nebo obsah dotazů hledání uživatele. Na rozdíl od programů typu Trojan-Spy adware odesílá informace vývojáři se souhlasem uživatele.

- Automatické vytáčení

Podkategorie: legální software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Úroveň nebezpečí: střední

Většina těchto aplikací je užitečná, takže je používá množství uživatelů. Tyto aplikace zahrnují klienty IRC, automatické vytáčení, programy pro stahování souborů, monitory aktivity počítačových systémů, nástroje pro správu hesel a internetové servery pro FTP, HTTP a Telnet.

Pokud však útočníci získají přístup k těmto programům nebo pokud je nasadí do počítače uživatele, mohou být některé funkce aplikace použity k narušení bezpečnosti.

Tyto aplikace se z hlediska funkcí liší. Jejich typy jsou popsány v následující tabulce.

Typ	Název	Popis
Client-IRC	Klienti internetových konverzací	Uživatelé instalují tyto programy, aby mohli komunikovat s lidmi v systému IRC (Internet Relay Chats). Útočníci je používají k šíření malwaru.
Dialer	Automatické vytáčení	Mohou navázat telefonická připojení přes modem ve skrytém režimu.
Downloader	Programy pro stahování	Mohou stahovat soubory z webových stránek ve skrytém režimu.
Monitor	Programy pro monitorování	Umožňují monitorování počítače, ve kterém jsou nainstalovány (zjištění, které aplikace jsou aktivní a jak si vyměňují data s aplikacemi nainstalovanými v jiných počítačích).
PSWTool	Nástroje pro obnovení hesla	Umožňují zobrazit a obnovit zapomenutá hesla. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem.
RemoteAdmin	Programy pro vzdálenou správu	Jsou často využívány správci systému. Tyto programy umožňují získat přístup k rozhraní vzdáleného počítače za účelem jeho sledování a správy. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem: monitorovat a spravovat vzdálené počítače. Legální programy pro vzdálenou správu se liší od trojských koňů typu Zadní vrátka pro vzdálenou správu. Trojské koně mohou proniknout do operačního systému nezávisle a nainstalovat se do něj. Legální programy to učinit nemohou.
Server-FTP	Servery FTP	Fungují jako servery FTP. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru FTP.
Server-Proxy	Proxy servery	Fungují jako proxy servery. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
Server-Telnet	Servery Telnet	Fungují jako servery Telnet. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru Telnet.
Server-Web	Webové servery	Fungují jako webové servery. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru HTTP.
RiskTool	Nástroje pro	Poskytují uživateli další možnosti při práci s vlastním počítačem

	práci na místním počítači	uživatele. Nástroje umožňují uživateli skrýt soubory nebo okna aktivních aplikací a ukončit aktivní procesy.
NetTool	Síťové nástroje	Poskytují uživateli další možnosti při práci s dalšími počítači v síti. Tyto nástroje umožňují jejich restart, zjištění otevřených portů a spuštění aplikací, které jsou v počítačích nainstalovány.
Client-P2P	Klienti sítě P2P	Umožňují práci v síti P2P. Útočníci je mohou používat k šíření malwaru.
Client-SMTP	Klienti SMTP	Odesílají e-mailové zprávy bez vědomí uživatele. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
WebToolbar	Webové panely nástrojů	Přidávají panely nástrojů do rozhraní jiných aplikací, aby bylo možné používat vyhledávače.
FraudTool	Pseudo programy	Vydávají se za jiné programy. Například existují pseudo antivirové programy, které zobrazují zprávy o zjištění malwaru. Ve skutečnosti však nic nenašly ani nedezinfikovaly.

- Další software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Podkategorie: legální software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Úroveň nebezpečí: střední

Většina těchto aplikací je užitečná, takže je používá množství uživatelů. Tyto aplikace zahrnují klienty IRC, automatické vytáčení, programy pro stahování souborů, monitory aktivity počítačových systémů, nástroje pro správu hesel a internetové servery pro FTP, HTTP a Telnet.

Pokud však útočníci získají přístup k těmto programům nebo pokud je nasadí do počítače uživatele, mohou být některé funkce aplikace použity k narušení bezpečnosti.

Tyto aplikace se z hlediska funkcí liší. Jejich typy jsou popsány v následující tabulce.

Typ	Název	Popis
Client-IRC	Klienti internetových konverzací	Uživatelé instalují tyto programy, aby mohli komunikovat s lidmi v systému IRC (Internet Relay Chats). Útočníci je používají k šíření malwaru.
Dialer	Automatické vytáčení	Mohou navázat telefonická připojení přes modem ve skrytém režimu.
Downloader	Programy pro stahování	Mohou stahovat soubory z webových stránek ve skrytém režimu.
Monitor	Programy pro monitorování	Umožňují monitorování počítače, ve kterém jsou nainstalovány (zjištění, které aplikace jsou aktivní a jak si vyměňují data s aplikacemi nainstalovanými v jiných počítačích).
PSWTool	Nástroje pro obnovení hesla	Umožňují zobrazit a obnovit zapomenutá hesla. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem.
RemoteAdmin	Programy pro vzdálenou správu	Jsou často využívány správci systému. Tyto programy umožňují získat přístup k rozhraní vzdáleného počítače za účelem jeho sledování a správy. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem: monitorovat a spravovat vzdálené počítače. Legální programy pro vzdálenou správu se liší od trojských koňů typu Zadní vrátka pro vzdálenou správu. Trojské koně mohou proniknout do operačního systému nezávisle a nainstalovat se do něj. Legální programy to učinit nemohou.
Server-FTP	Servery FTP	Fungují jako servery FTP. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru FTP.
Server-Proxy	Proxy servery	Fungují jako proxy servery. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
Server-Telnet	Servery Telnet	Fungují jako servery Telnet. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru Telnet.
Server-Web	Webové servery	Fungují jako webové servery. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru HTTP.
RiskTool	Nástroje pro	Poskytují uživateli další možnosti při práci s vlastním počítačem

	práci na místním počítači	uživatele. Nástroje umožňují uživateli skrýt soubory nebo okna aktivních aplikací a ukončit aktivní procesy.
NetTool	Síťové nástroje	Poskytují uživateli další možnosti při práci s dalšími počítači v síti. Tyto nástroje umožňují jejich restart, zjištění otevřených portů a spuštění aplikací, které jsou v počítačích nainstalovány.
Client-P2P	Klienti sítě P2P	Umožňují práci v síti P2P. Útočníci je mohou používat k šíření malwaru.
Client-SMTP	Klienti SMTP	Odesílají e-mailové zprávy bez vědomí uživatele. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
WebToolbar	Webové panely nástrojů	Přidávají panely nástrojů do rozhraní jiných aplikací, aby bylo možné používat vyhledávače.
FraudTool	Pseudo programy	Vydávají se za jiné programy. Například existují pseudo antivirové programy, které zobrazují zprávy o zjištění malwaru. Ve skutečnosti však nic nenašly ani nedezinfikovaly.

- **Komprimované objekty, jejichž komprimace může sloužit k ochraně škodlivého kódu**

  Aplikace Kaspersky Endpoint Security kontroluje komprimované objekty a rozbalovací modul v (samorozbalovacích) SFX archivech.

  Aby bylo možné skrýt nebezpečné programy před antivirovými aplikacemi, útočníci je archivují pomocí speciálních komprimačních programů nebo vytvoří několikrát komprimované soubory.

  Analytikové společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

  Pokud aplikace Kaspersky Endpoint Security detekuje takový komprimační program v souboru, soubor pravděpodobně obsahuje škodlivou aplikaci nebo aplikaci, kterou lze použít zločinným způsobem k poškození počítače nebo osobních dat.

  Aplikace Kaspersky Endpoint Security rozlišuje následující typy programů:

  - *Komprimované soubory, které mohou způsobit škodu* – používají se k balení malwaru, například virů, červů a trojských koňů.
  - *Mnohonásobně komprimované soubory* (střední úroveň rizika) – objekt byl zkomprimován třikrát jedním nebo více komprimačními nástroji.

- **Mnohonásobně komprimované soubory**

Aplikace Kaspersky Endpoint Security kontroluje komprimované objekty a rozbalovací modul v (samorozbalovacích) SFX archivech.

Aby bylo možné skrýt nebezpečné programy před antivirovými aplikacemi, útočníci je archivují pomocí speciálních komprimačních programů nebo vytvoří několikrát komprimované soubory.

Analytikové společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

Pokud aplikace Kaspersky Endpoint Security detekuje takový komprimační program v souboru, soubor pravděpodobně obsahuje škodlivou aplikaci nebo aplikaci, kterou lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Aplikace Kaspersky Endpoint Security rozlišuje následující typy programů:

- *Komprimované soubory, které mohou způsobit škodu* – používají se k balení malwaru, například virů, červů a trojských koňů.
- *Mnohonásobně komprimované soubory* (střední úroveň rizika) – objekt byl zkomprimován třikrát jedním nebo více komprimačními nástroji.

4. Uložte změny.

Povolení nebo zakázání technologie pokročilé dezinfekce

Pokud aplikace Kaspersky Endpoint Security nemůže zastavit provádění malwaru, můžete použít technologii Pokročilá dezinfekce. Pokročilá dezinfekce je standardně zakázána, protože používá značné množství výpočetních prostředků. Pokročilou dezinfekci tak můžete povolit, pouze pokud pracujete s aktivními hrozbami.

Pokročilá dezinfekce funguje jinak u pracovních stanic a serverů. Chcete-li používat tuto technologii na serverech, musíte ve vlastnostech úlohy *Antivirová kontrola* povolit okamžitou pokročilou dezinfekci. Tato podmínka není nutná pro používání této technologie na pracovních stanicích.

Povolení nebo zakázání technologie Pokročilá dezinfekce:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně s nastavením aplikace vyberte část **Obecné**.
3. V části **Režim ochrany** pomocí zaškrtávacího políčka **Povolit technologii pokročilé dezinfekce** povolte nebo zakažte technologii pokročilé dezinfekce.
4. Uložte změny.

Uživatel tak nemůže využívat většinu funkcí operačního systému, když probíhá pokročilá dezinfekce. Po dokončení dezinfekce se počítač restartuje.

Povolení nebo zakázání režimu úspory energie

Postup povolení nebo zakázání režimu úspory energie:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Hrozby a výjimky**.
3. V části **Výkon** zaškrtnutím políčka **Odložit naplánované úlohy při napájení z baterie** povolte nebo zakažte režim úspory energie.

   Když je režim úspory energie povolen a počítač je napájen z baterie, následující úlohy nebudou spuštěny ani v případě, že byly naplánované:

   - úloha Aktualizace;
   - úloha Úplná kontrola;
   - úloha Kontrola kritických oblastí;
   - úloha Vlastní kontrola;
   - úloha Kontrola integrity.
4. Uložte změny.

Povolení nebo zakázání uvolnění prostředků pro jiné aplikace

Postup povolení nebo zakázání uvolnění prostředků pro jiné aplikace:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.
2. V okně s nastavením aplikace vyberte část **Obecné**.
3. V části **Výkon** pomocí zaškrtávacího políčka **Při zatížení přenechat zdroje ostatním aplikacím** povolíte nebo zakážete přenechávání prostředků jiným aplikacím.

   Když je nastaveno uvolnění prostředků pro jiné aplikace, aplikace Kaspersky Endpoint Security odloží naplánované úlohy, které zpomalují jiné aplikace:

   - úloha Aktualizace;
   - úloha Úplná kontrola;
   - úloha Kontrola kritických oblastí;
   - úloha Vlastní kontrola;
   - úloha Kontrola integrity.

   Aplikace ve výchozím nastavení uvolňuje prostředky pro jiné aplikace.
4. Uložte změny.

Vytvoření nebo použití konfiguračního souboru

Konfigurační soubor s nastavením aplikace Kaspersky Endpoint Security umožňuje provádět následující úlohy:

- Provádět místní instalaci aplikace Kaspersky Endpoint Security prostřednictvím příkazového řádku s předdefinovanými nastaveními.

  Aby to bylo možné, musíte konfigurační soubor uložit do stejné složky, ve které se nachází distribuční balíček.

- Provádět vzdálenou instalaci aplikace Kaspersky Endpoint Security prostřednictvím aplikace Kaspersky Security Center s předdefinovanými nastaveními.

- Přenášet nastavení aplikace Kaspersky Endpoint Security z jednoho počítače do druhého.

Postup vytvoření konfiguračního souboru:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Správa nastavení**.
3. Klikněte na tlačítko **Exportovat**.
4. V okně, které se otevře, určete cestu k umístění, do kterého chcete uložit konfigurační soubor, a zadejte jeho název.

   Pokud chcete konfigurační soubor použít k místní nebo vzdálené instalaci aplikace Kaspersky Endpoint Security, musíte ho pojmenovat install.cfg.

5. Klikněte na tlačítko **Uložit**.

Postup importu nastavení aplikace Kaspersky Endpoint Security z konfiguračního souboru:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Správa nastavení**.
3. Klikněte na tlačítko **Importovat**.
4. V okně, které se otevře, zadejte cestu ke konfiguračnímu souboru.
5. Klikněte na tlačítko **Otevřít**.

Všechny hodnoty nastavení aplikace Kaspersky Endpoint Security budou určeny podle vybraného konfiguračního souboru.

Obnovení výchozího nastavení aplikace

Nastavení doporučené společností Kaspersky pro aplikaci Kaspersky Endpoint Security můžete kdykoli obnovit. Po obnovení nastavení bude pro všechny součásti ochrany nastavena **doporučená** úroveň zabezpečení.

Postup obnovení výchozího nastavení aplikace:

1. V dolní části okna aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnosti **Správa nastavení**.
3. Klikněte na tlačítko **Obnovit**.
4. Klikněte na tlačítko **Uložit**.

Zasílání zpráv mezi uživateli a správcem

Součásti Kontrola aplikací, Kontrola zařízení, Kontrola webu a Adaptivní kontrola anomálií umožňují uživatelům v síti LAN s počítači s nainstalovanou aplikací Kaspersky Endpoint Security odesílat zprávy správci.

V následujících případech může být zapotřebí, aby uživatel odeslal zprávu správci místní podnikové sítě:

- Kontrola zařízení zablokovala přístup k zařízení.

  Šablona zprávy pro žádost o přístup k blokovanému zařízení je k dispozici v rozhraní aplikace Kaspersky Endpoint Security v části Kontrola zařízení.

- Součást Kontrola aplikací zablokovala spuštění aplikace.

  Šablona zprávy pro žádost o povolení ke spuštění zablokované aplikace je k dispozici v rozhraní aplikace Kaspersky Endpoint Security v části Kontrola aplikací.

- Kontrola webu zablokovala přístup k webovému prostředku.

  Šablona zprávy pro žádost o přístup k zablokovanému webovému prostředku je k dispozici v rozhraní aplikace Kaspersky Endpoint Security v části Kontrola webu.

Metody zasílání zpráv a použité šablony závisí na tom, zda existují aktivní zásady aplikace Kaspersky Security Center používané v počítači, ve kterém je nainstalována aplikace Kaspersky Endpoint Security, a zda je k dispozici připojení k administračnímu serveru Kaspersky Security Center. Možné jsou následující scénáře:

- Pokud v počítači s aplikací Kaspersky Endpoint Security nejsou používány zásady aplikace Kaspersky Security Center, bude zpráva od uživatele odeslána správci místní sítě e-mailem.

  Pole zprávy jsou vyplněna hodnotami z polí šablony definované v místním rozhraní aplikace Kaspersky Endpoint Security.

- Pokud jsou v počítači s aplikací Kaspersky Endpoint Security používány zásady aplikace Kaspersky Security Center, bude standardní zpráva odeslána na server pro správu aplikace Kaspersky Security Center.

  V takovém případě bude možné zprávy uživatele zobrazit v úložišti událostí Kaspersky Security Center (viz pokyny níže). Pole zprávy jsou vyplněna hodnotami z polí šablony definované v zásadách aplikace Kaspersky Security Center.

- Pokud jsou v počítači s aplikací Kaspersky Security Center používány zásady „mimo kancelář“ aplikace Kaspersky Security Center, způsob odesílání zpráv závisí na tom, zda existuje spojení s aplikací Kaspersky Security Center.

  - Pokud je spojení s aplikací Kaspersky Security Center navázáno, aplikace Kaspersky Endpoint Security odešle standardní zprávu do administračního serveru Kaspersky Security Center.

  - Pokud spojení s aplikací Kaspersky Security Center chybí, bude zpráva od uživatele odeslána správci místní sítě e-mailem.

  V obou případech budou pole zprávy vyplněna hodnotami z polí šablony definované v zásadách aplikace Kaspersky Security Center.

Postup zobrazení uživatelské zprávy v úložišti událostí aplikace Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. V uzlu **Administration Server** ve stromu konzole pro správu vyberte kartu **Events**.

   V pracovním prostoru aplikace Kaspersky Security Center se zobrazí všechny události, ke kterým došlo během provozu aplikace Kaspersky Endpoint Security, včetně zpráv pro správce obdržených od uživatelů v síti LAN.

3. Chcete-li nakonfigurovat filtr událostí, v rozevíracím seznamu **Selection events** vyberte možnost **User requests**.

4. Vyberte zprávu, která se odešle správci.

5. Klikněte na tlačítko **Open event properties window** v pravé části pracovního prostoru konzole pro správu.

Šifrování dat

Aplikace Kaspersky Endpoint Security umožňuje šifrovat soubory a složky, které jsou uložené na místních a vyměnitelných jednotkách, nebo také celé vyměnitelné jednotky a pevné disky. Šifrování dat minimalizuje riziko úniků informací, k nimž může dojít při ztrátě nebo odcizení přenosného počítače, vyměnitelné jednotky nebo pevného disku nebo při přístupu neautorizovaných uživatelů nebo aplikací k datům. Aplikace Kaspersky Endpoint Security používá šifrovací algoritmus AES (Advanced Encryption Standard).

Jestliže skončila platnost licence, aplikace nešifruje nová data a stará šifrovaná data zůstanou zašifrovaná a je možné je používat. V tomto případě vyžaduje šifrování nových dat aktivaci aplikace pomocí nové licence, která dovoluje použití šifrování.

Jestliže skončila platnost vaší licence nebo došlo k porušení podmínek licenční smlouvy s koncovým uživatelem nebo byl odebrán licenční klíč, aplikace Kaspersky Endpoint Security nebo součásti šifrování, nelze zaručit stav šifrování u dříve zašifrovaných souborů. Je to způsobeno tím, že některé aplikace, například Microsoft Office Word, vytváří během úprav souborů dočasnou kopii. Při uložení původního souboru je původní soubor nahrazen dočasnou kopií. V důsledku toho zůstane takový soubor v počítači, v němž není k dispozici žádná funkce šifrování nebo funkce šifrování není dostupná, nezašifrovaný.

Aplikace Kaspersky Endpoint Security nabízí následující možnosti ochrany dat:

- **Šifrování na úrovni souborů na místních discích počítače**. Můžete zkompilovat seznamy souborů podle přípony nebo skupiny přípon a seznamy složek uložených na místních počítačových discích a vytvořit pravidla šifrování souborů vytvořených určitými aplikacemi. Po použití zásad aplikace Kaspersky Security Center zašifruje a dešifruje následující soubory:
  - Soubory jednotlivě přidané na seznamy pro šifrování a dešifrování.
  - Soubory uložené ve složkách přidaných na seznamy pro šifrování a dešifrování.
  - Soubory vytvořené samostatnými aplikacemi.
- **Šifrování vyměnitelných jednotek**. Můžete zadat výchozí pravidlo šifrování, podle kterého aplikace provede stejnou akci u všech vyměnitelných jednotek, nebo zadat pravidla šifrování pro jednotlivé vyměnitelné jednotky.

  Výchozí pravidlo šifrování má nižší prioritu než pravidla šifrování vytvořená pro jednotlivé vyměnitelné jednotky. Pravidla šifrování vytvořená pro vyměnitelné jednotky zadaného modelu zařízení mají nižší prioritu než pravidla šifrování vytvořená pro vyměnitelné jednotky se zadaným ID zařízení.

  Aplikace Kaspersky Endpoint Security při volbě pravidla šifrování pro soubory na vyměnitelné jednotce kontroluje, zda jsou model nebo ID zařízení známé. Aplikace potom provede jednu z těchto akcí:
  - Pokud je znám jen model zařízení, aplikace použije pravidlo šifrování (pokud nějaké existuje) vytvořené pro vyměnitelné jednotky určitého modelu zařízení.
  - Pokud je známo jen ID zařízení, aplikace použije pravidlo šifrování (pokud nějaké existuje) vytvořené pro vyměnitelné jednotky s určitým ID zařízení.
  - Pokud jsou známy model i ID zařízení, aplikace použije pravidlo šifrování (pokud nějaké existuje) vytvořené pro vyměnitelné jednotky s určitým ID zařízení. Pokud žádné takové pravidlo neexistuje, ale existuje pravidlo šifrování vytvořené pro vyměnitelné jednotky určitého modelu zařízení, aplikace použije toto pravidlo. Pokud není zadáno žádné pravidlo šifrování pro určité ID zařízení ani pro určitý model zařízení, aplikace použije výchozí pravidlo šifrování.
  - Pokud není znám model zařízení ani jeho ID, aplikace použije výchozí pravidlo šifrování.

Aplikace vám umožní připravit vyměnitelnou jednotku pro použití šifrovaných dat, které jsou na ní uložené v mobilním režimu. Po povolení mobilního režimu získáte přístup k šifrovaným souborům na vyměnitelných jednotkách připojených k počítači bez funkce šifrování.

- **Správa pravidel přístupu aplikací k šifrovaným souborům**. Pro jakoukoli aplikaci můžete vytvořit pravidlo přístupu k šifrovaným souborů, které blokuje přístup k šifrovaným souborů nebo povoluje přístup k šifrovaným souborům pouze jako k šifrovanému textu, což je sekvence znaků získaná při šifrování.

- **Vytvoření šifrovaných balíčků**. Můžete vytvářet šifrované archivy a přístup k nim chránit pomocí hesla. Přístup k obsahu šifrovaných archivů lze získat jen po zadání hesel, která slouží k zabezpečení přístupu k těmto archivům. Tyto archivy je možné bezpečně přenášet po sítích nebo pomocí vyměnitelných jednotek.

- **Úplné šifrování disku**. Můžete vybrat technologii šifrování: Kaspersky Disk Encryption nebo BitLocker Drive Encryption (dále označována zkráceně jako „technologie BitLocker“).

  BitLocker je technologie, která je součástí operačního systému Windows. Pokud je počítač vybavený čipem TPM (Trusted Platform Module), technologie BitLocker jej použije k ukládání obnovovacích klíčů, které poskytují přístup k šifrovanému pevnému disku. Po spuštění počítače vyžádá technologie BitLocker obnovovací klíče pevného disku z čipu TPM a potom disk odemkne. Pro přístup k obnovovacím klíčům můžete nastavit použití hesla a/nebo PIN kódu.

  Můžete zadat výchozí pravidlo úplného šifrování disku a vytvořit seznam pevných disků, které mají být z šifrování vyloučeny. Aplikace Kaspersky Endpoint Security provádí úplné šifrování disku (každý sektor), jakmile se použijí zásady aplikace Kaspersky Security Center. Aplikace současně šifruje všechny logické oddíly pevných disků.

  Po zašifrování systémových pevných disků se musí uživatel při příštím spuštění počítače ověřit prostřednictvím ověřovacího agenta a až poté jsou zpřístupněna data na pevných discích a načten operační systém. Tato akce vyžaduje zadání hesla tokenu nebo čipové karty připojené k počítači nebo uživatelského jména a hesla účtu ověřovacího agenta, který byl vytvořen správcem místní sítě pomocí úlohy *Správa účtů ověřovacího agenta*. Tyto účty jsou založené na účtech systému Microsoft Windows, které uživatelé používají k přihlašování do operačního systému. Můžete také použít technologii SSO (Single Sign-On), která umožňuje automatické přihlášení k operačnímu systému pomocí uživatelského jména a hesla účtu ověřovacího agenta.

  > Pokud zazálohujete počítač a zašifrujete jeho data a potom obnovíte záložní kopii počítače a znovu zašifrujete data počítače, aplikace Kaspersky Endpoint Security vytvoří duplicitní účty ověřovacího agenta. Chcete-li duplicitní účty odebrat, je třeba použít nástroj klmover s klíčem `dupfix`. Nástroj klmover je součástí sestavy aplikace Kaspersky Security Center. Více informací o jeho fungování můžete najít v nápovědě k aplikaci Kaspersky Security Center.

  Přístup k šifrovaným pevným diskům je možný jen z počítačů, v nichž je nainstalována aplikace Kaspersky Endpoint Security s funkcí úplného šifrování disku. Toto opatření minimalizuje riziko úniků dat z šifrovaného pevného disku při pokusu o přístup z místa mimo místní síť společnosti.

K šifrování pevných disků a vyměnitelných jednotek můžete použít funkci **Zašifrovat pouze využité místo na disku**. Tuto funkci doporučujeme používat jen pro nová zařízení, která dosud nebyla použita. Pokud chcete použít šifrování na zařízení, které se již používá, doporučujeme zašifrovat celé zařízení. Zajistíte tím ochranu veškerých dat – i odstraněných dat, která mohou obsahovat čitelné informace.

Aplikace Kaspersky Endpoint Security před zahájením šifrování získá mapu sektorů souborového systému. První vlna šifrování zahrnuje sektory obsazené soubory v době, kdy je šifrování spuštěno. Druhá vlna šifrování zahrnuje sektory, v nichž byl proveden zápis po zahájení šifrování. Po dokončení šifrování jsou zašifrovány všechny sektory obsahující data.

Jakmile se šifrování dokončí a uživatel odstraní nějaký soubor, sektory, kde byl odstraněný soubor uložen, se uvolní k uložení nových dat na úrovni souborového systému, zůstanou však zašifrované. Když jsou tedy zapsány soubory do nového zařízení a zařízení je pravidelně šifrováno s povolenou funkcí **Zašifrovat pouze využité místo na disku**, budou po určité době zašifrovány všechny sektory.

Data potřebná k dešifrování souboru jsou poskytována administračním serverem Kaspersky Security Center, který kontroloval počítač v době šifrování. Pokud byl počítač se šifrovanými objekty z nějakého důvodu spravován jiným serverem pro správu, můžete získat přístup k šifrovaným datům jedním z následujících způsobů:

- Servery pro správ ve stejné hierarchii:
  - Nemusíte podnikat žádné další kroky. Uživatel si zachová přístup k šifrovaným objektům. Šifrovací klíče jsou distribuovány na všechny servery pro správu.
- Samostatné servery pro správu:
  - Požádejte o přístup k šifrovaným objektům správce sítě LAN.
  - Obnovte data v šifrovaných zařízeních pomocí nástroje pro obnovení.
  - Obnovte konfiguraci serveru pro správu Kaspersky Security Center, který kontroloval počítač v době šifrování, pomocí záložní kopie a použijte tuto konfiguraci na administračním serveru, který nyní kontroluje počítač se šifrovanými objekty.

Pokud k šifrovaným datům není přístup, postupujte podle zvláštních pokynů pro práci se šifrovanými daty (Obnovení přístupu k šifrovaným souborům, Práce s šifrovanými zařízeními v případě, že není k dispozici žádný přístup k nim).

Omezení funkce šifrování

Šifrování dat má následující omezení:

- Během šifrování aplikace vytváří servisní soubory. K jejich uložení je třeba přibližně 0,5 % volného místa na pevném disku. Pokud na pevném disku není dostatek volného místa bez fragmentace, šifrování nebude spuštěno, dokud nebude uvolněn dostatek místa.
- Veškeré součásti pro šifrování dat můžete spravovat v konzole pro správu aplikace Kaspersky Security Center a ve webové konzole aplikace Kaspersky Security Center 12. V cloudové konzole aplikace Kaspersky Security Center můžete spravovat pouze nástroj Bitlocker.
- Šifrování dat je k dispozici pouze při použití aplikace Kaspersky Endpoint Security se systémem pro správu Kaspersky Security Center nebo cloudovou konzolou Kaspersky Security Center (pouze BitLocker). Šifrování dat při používání aplikace Kaspersky Endpoint Security v režimu offline není možné, protože aplikace Kaspersky Endpoint Security ukládá šifrovací klíče v aplikaci Kaspersky Security Center.
- Pokud je aplikace Kaspersky Endpoint Security nainstalována v počítači, ve kterém je spuštěn systém Microsoft Windows pro souborové servery, je k dispozici pouze úplné šifrování disku pomocí technologie BitLocker Drive Encryption. Jestliže je aplikace Kaspersky Endpoint Security nainstalována v počítači, ve kterém je spuštěn systém Windows pro pracovní stanice, funkce šifrování dat je plně dostupná.

Úplné šifrování disku pomocí technologie Kaspersky Disk Encryption není k dispozici pro pevné disky, které nesplňují požadavky na hardware a software.

Kompatibilita mezi funkcemi úplného šifrování disku aplikací Kaspersky Endpoint Security a Kaspersky Anti-Virus pro UEFI není podporována. Aplikace Kaspersky Anti-Virus pro UEFI se spustí před načtením operačního systému. Při použití šifrování celého disku aplikace zjistí nepřítomnost nainstalovaného operačního systému v počítači. Provoz aplikace Kaspersky Anti-Virus pro UEFI proto skončí chybou. Šifrování na úrovni souborů (FLE) činnost aplikace Kaspersky Anti-Virus pro UEFI neovlivňuje.

Aplikace Kaspersky Endpoint Security podporuje následující konfigurace:

- Jednotky HDD, SSD a USB.

  Technologie Kaspersky Disk Encryption (FDE) podporuje práci s SSD při zachování výkonu a životnosti disků SSD.

- Jednotky připojené přes sběrnici: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- Nevyměnitelné disky připojené přes sběrnici SD nebo MMC.
- Jednotky s 512bajtovými sektory.
- Jednotky s 4096bajtovými sektory, které emulují 512 bajtů.
- Jednotky s následujícím typem oddílů: GPT, MBR a VBR (vyměnitelné jednotky).
- Integrovaný software standardu UEFI 64 a Legacy BIOS.
- Integrovaný software standardu UEFI s podporou Secure Boot.

  Secure Boot je technologie určená k ověřování digitálních podpisů pro aplikace a zavaděče UEFI. Secure Boot blokuje spouštění aplikací a zavaděčů UEFI, které jsou nepodepsané nebo podepsané neznámými vydavateli. Kaspersky Disk Encryption (FDE) funkci Secure Boot plně podporuje. Ověřovací agent je podepsán certifikátem Microsoft Windows UEFI Driver Publisher.

  Na některých zařízeních (například Microsoft Surface Pro a Microsoft Surface Pro 2) může být ve výchozím nastavení nainstalován zastaralý seznam certifikátů pro ověření digitálního podpisu. Před zašifrováním jednotky musíte seznam certifikátů aktualizovat.

- Integrovaný software standardu UEFI s podporou Fast Boot.

  Fast Boot je technologie, která pomáhá rychlejšímu spuštění počítače. Když je technologie Fast Boot povolena, počítač obvykle načte pouze minimální sadu ovladačů UEFI potřebných pro spuštění operačního systému. Když je technologie Fast Boot povolena, USB klávesnice, myši, USB tokeny, touchpady a dotykové obrazovky nemusí fungovat, když je spuštěn Ověřovací agent.

  Chcete-li používat Kaspersky Disk Encryption (FDE), doporučujeme technologii Fast Boot zakázat. K otestování funkce Kaspersky Disk Encryption (FDE) můžete použít nástroj FDE Test Utility.

Aplikace Kaspersky Endpoint Security nepodporuje následující konfigurace:

- nástroj pro zavádění se nachází na jednom disku, zatímco operační systém je umístěn na jiném disku;
- systém obsahuje integrovaný software standardu UEFI 32;
- systém má technologii Intel® Rapid Start a disky zahrnující oddíl pro hibernaci, i když je technologie Intel® Rapid Start zakázána;
- disky ve formátu MBR s více než 10 rozšířenými oddíly;
- systém má soubor swap nacházející se na nesystémovém disku;
- systém s více spouštěcími body a několika souběžně nainstalovanými operačními systémy;
- dynamické oddíly (podporovány jsou pouze primární oddíly);
- disky s méně než 0,5 % volného nefragmentovaného místa;

- disky s velikostí sektoru jinou než 512 bajtů nebo 4096 bajtů emulující 512 bajtů;
- hybridní disky;
- systém má zavaděče třetích stran;
- jednotky s komprimovanými adresáři NTFS.
- Technologie Kaspersky Disk Encryption (FDE) je nekompatibilní s jinými technologiemi šifrování celého disku (jako je BitLocker, McAfee Drive Encryption a WinMagic SecureDoc).
- Technologie Kaspersky Disk Encryption (FDE) je nekompatibilní s technologií Express Cache.
- Vytváření, odstraňování a úpravy oddílů na šifrované jednotce není podporováno. Mohli byste přijít o data.
- Formátování systému souborů není podporováno. Mohli byste přijít o data.

  Pokud potřebujete naformátovat jednotku, která byla zašifrována pomocí technologie Kaspersky Disk Encryption (FDE), naformátujte jednotku v počítači, který nemá nainstalovánu aplikaci Kaspersky Endpoint Security pro systém Windows, a použijte pouze úplné šifrování disku.

  Šifrovaná jednotka, která je naformátována pomocí možnosti rychlého formátování, může být při příštím připojení k počítači, na kterém je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows, omylem identifikována jako šifrovaná. Uživatelská data nebudou k dispozici.
- Ověřovací agent nepodporuje více než 100 účtů.
- Technologie SSO (Single Sign-On) je nekompatibilní s jinými technologiemi vývojářů třetích stran.
- Technologie Kaspersky Disk Encryption (FDE) není podporována v následujících modelech zařízení:
  - Dell Latitude E6410 (režim UEFI)
  - HP Compaq nc8430 (režim Legacy BIOS)
  - Lenovo Think Center 8811 (starší režim BIOS)
- Ověřovací agent nepodporuje práci s USB tokeny, když je povolena podpora Legacy USB. V počítači bude možné pouze ověřování založené na heslech.
- Při šifrování jednotky v režimu Legacy BIOS se doporučuje povolit podporu Legacy USB na následujících modelech zařízení:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300

- Dell Studio 1537
- Dell Studio 1569
- Dell Vostro 1310
- Dell Vostro 1320
- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- Počítač HP Compaq dx2450 Microtower
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (základní deska)

Změna délky šifrovacího klíče (AES56/AES256)

Aplikace Kaspersky Endpoint Security používá šifrovací algoritmus AES (Advanced Encryption Standard). Aplikace Kaspersky Endpoint Security podporuje šifrovací algoritmus AES s efektivní délkou klíče 256 nebo 56 bitů. Algoritmus šifrování dat závisí na šifrovací knihovně AES, která je součástí distribučního balíčku: *silné šifrování (AES256)* nebo *lehké šifrování (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.

Změna délky šifrovacího klíče je k dispozici pouze pro aplikaci Kaspersky Endpoint Security 11.2.0 nebo novější.

Změna délky šifrovacího klíče se skládá z následujících kroků:

1. Než začnete měnit délku šifrovacího klíče, dešifrujte objekty, které aplikace Kaspersky Endpoint Security dříve zašifrovala:

   a. Dešifrujte pevné disky.

   b. Dešifrujte soubory na místních jednotkách.

   c. Dešifrujte vyměnitelné jednotky.

   Po změně délky šifrovacího klíče se objekty zašifrované dříve stanou nedostupnými.

2. Odeberte aplikaci Kaspersky Endpoint Security.

3. Nainstalujte aplikaci Kaspersky Endpoint Security z distribučního balíčku aplikace Kaspersky Endpoint Security obsahujícího jinou knihovnu šifrování.

Délku šifrovacího klíče můžete také změnit upgradováním aplikace. Délku klíče lze změnit upgradem aplikace, pouze pokud jsou splněny následující podmínky:

- V počítači je nainstalována aplikace Kaspersky Endpoint Security verze 10 Service Pack 2 nebo novější.
- V počítači nejsou nainstalovány součásti šifrování dat (šifrování na úrovni souborů, úplné šifrování disku).

  Ve výchozím nastavení nejsou součásti šifrování dat součástí aplikace Kaspersky Endpoint Security. Součást BitLocker Management neovlivňuje změnu délky šifrovacího klíče.

Chcete-li změnit délku šifrovacího klíče, z distribučního balíčku obsahujícího potřebnou knihovnu šifrování spusťte soubor kes_win.msi nebo setup_kes.exe. Aplikaci můžete také vzdáleně upgradovat pomocí instalačního balíčku.

Délku šifrovacího klíče nelze měnit pomocí distribučního balíčku stejné verze aplikace, která je na vašem počítači nainstalována, aniž by byla aplikace nejprve odinstalována.

Kaspersky Disk Encryption

Technologie Kaspersky Disk Encryption je k dispozici pouze pro počítače s operačním systémem Windows pro pracovní stanice. U počítačů s operačním systémem Windows pro servery použijte technologii BitLocker Drive Encryption.

Aplikace Kaspersky Endpoint Security podporuje úplné šifrování disku v souborových systémech FAT32, NTFS a exFat.

Aplikace spouští před zahájením úplného šifrování disku řadu kontrol k určení, zda lze zařízení šifrovat, což zahrnuje i kontrolu kompatibility systémového pevného disku s šifrovacími součástmi ověřovacího agenta nebo nástroje BitLocker. Aby bylo možné ověřit kompatibilitu, počítač musí být restartován. Po restartu počítače provede aplikace všechny potřebné kontroly automaticky. Jestliže proběhne kontrola kompatibility úspěšně, úplné šifrování disku se spustí po načtení operačního systému a spuštění aplikace. Pokud je zjištěno, že systémový pevný disk není kompatibilní s šifrovacími součástmi ověřovacího agenta nebo BitLocker, je třeba počítač restartovat stisknutím tlačítka pro reset hardwaru. Aplikace Kaspersky Endpoint Security zaznamená informace o nekompatibilitě. Na základě těchto informací aplikace nespustí úplné šifrování disku při spouštění operačního systému. Informace o této události jsou zaznamenány do zpráv aplikace Kaspersky Security Center.

Pokud se konfigurace hardwaru počítače změní, informace o nekompatibilitě zaznamenané aplikací během předchozí kontroly je třeba odstranit, aby bylo možné zkontrolovat kompatibilitu systémového pevného disku s šifrovacími součástmi ověřovacího agenta a BitLocker. K tomu je třeba před úplným šifrováním disku zadat na příkazovém řádku příkaz `avp pbatestreset`. Pokud se operační systém nenačte po kontrole kompatibility systémového pevného disku s ověřovacím agentem, je třeba odebrat objekty a data, které zbyly po testovacím provozu ověřovacího agenta, pomocí nástroje pro obnovení a potom spustit aplikaci Kaspersky Endpoint Security a znovu provést příkaz `avp pbatestreset`.

Aplikace Kaspersky Endpoint Security po spuštění úplného šifrování disku zašifruje všechna data zapsaná na pevné disky.

Jestliže uživatel vypne nebo restartuje počítač během úplného šifrování disku, před příštím spuštěním operačního systému se načte ověřovací agent. Po úspěšném ověření pomocí ověřovacího agenta a spuštění operačního systému obnoví aplikace Kaspersky Endpoint Security úplné šifrování disku.

Jestliže se během úplného šifrování disku přepne operační systém do režimu hibernace, po ukončení režimu hibernace se načte ověřovací agent. Po úspěšném ověření pomocí ověřovacího agenta a spuštění operačního systému obnoví aplikace Kaspersky Endpoint Security úplné šifrování disku.

Jestliže během úplného šifrování disku přejde operační systém do režimu spánku, aplikace Kaspersky Endpoint Security obnoví úplné šifrování disku, jakmile dojde k ukončení režimu spánku (ověřovací agent se nenačte).

Ověření uživatele ověřovacím agentem lze provést dvěma způsoby:

- Zadejte název a heslo účtu ověřovacího agenta, který byl vytvořen správcem sítě LAN pomocí nástrojů aplikace Kaspersky Security Center.
- Zadejte heslo tokenu nebo čipové karty připojené k počítači.

  Použití tokenu nebo čipové karty bude k dispozici, pouze pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES256. Pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES56, přiřazení souboru elektronického certifikátu k příkazu bude zamítnuto.

Ověřovací agent podporuje rozložení klávesnice pro následující jazyky:

- Angličtina (Velká Británie)
- Angličtina (USA)
- Arabština (Alžírsko, Maroko, Tunisko, rozložení AZERTY)
- Španělština (Latinská Amerika)
- Italština
- Němčina (Německo a Rakousko)

- Němčina (Švýcarsko)
- Portugalština (Brazílie, rozložení ABNT2)
- Ruština (pro klávesnice IBM/Windows se 105 klávesami s rozložením QWERTY)
- Turečtina (rozložení QWERTY)
- Francouzština (Francie)
- Francouzština (Švýcarsko)
- Francouzština (Belgie, rozložení AZERTY)
- Japonština (pro klávesnice se 106 klávesami s rozložením QWERTY)

Rozložení klávesnice je k dispozici v ověřovacím agentovi, pokud toto rozložení bylo přidáno do nastavení jazyka a místních standardů operačního systému a je k dispozici na úvodní obrazovce systému Microsoft Windows.

Pokud název účtu ověřovacího agenta obsahuje symboly, které nelze zadat pomocí rozložení klávesnice dostupného v rámci ověřovacího agenta, přístup k šifrovaným pevným diskům je možný jen po jejich obnovení pomocí nástroje pro obnovení nebo po obnovení názvu a hesla účtu ověřovacího agenta.

Zvláštní funkce šifrování jednotky SSD

Aplikace podporuje šifrování disků SSD, hybridních disků SSHD a disků s funkcí Intel Smart Response. Aplikace nepodporuje šifrování disků pomocí funkce Intel Rapid Start. Před šifrováním takové jednotky deaktivujte funkci Intel Rapid Start.

Šifrování disků SSD má následující speciální funkce:

- Pokud je jednotka SSD nová a neobsahuje žádná důvěrná data, povolte šifrování pouze obsazeného prostoru. To vám umožní přepsat příslušné sektory jednotek.
- Pokud se disk SSD používá a obsahuje důvěrná data, vyberte jednu z následujících možností:
  - Úplně disk SSD vymažte (Secure Erase), nainstalujte operační systém a spusťte šifrování disku SSD s možností šifrování povoleného pouze obsazeného místa.
  - Spusťte šifrování disku SSD s možností šifrování deaktivovaného pouze obsazeného prostoru.

Šifrování disku SSD vyžaduje 5–10 GB volného místa. Požadavky na volné místo pro ukládání dat pro správu šifrování jsou uvedeny v tabulce níže.

Požadavky na volné místo pro ukládání dat pro správu šifrování

Velikost disku SSD (GB)	Volné místo na primárním oddílu disku SSD (MB)	Volné místo na sekundárním oddílu disku SSD (MB)
128	250	64
256	250	640
512	300	128

Úplné šifrování disku pomocí technologie Kaspersky Disk Encryption

Před spuštěním úplného šifrování disku se doporučuje ověřit, že počítač není infikovaný. To můžete provést spuštěním úlohy Úplná kontrola nebo Kontrola kritických oblastí. Provedení úplného šifrování disku v počítači, který je infikovaný rootkitem, může způsobit nefunkčnost počítače.

Postup provedení úplného šifrování disku pomocí technologie Kaspersky Disk Encryption:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.
6. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **Kaspersky Disk Encryption**.

   Technologii Kaspersky Disk Encryption nelze použít, jestliže počítač obsahuje pevné disky, které byly šifrované nástrojem BitLocker.

7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Šifrovat všechny pevné disky**.

   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování všech pevných disků načíst pouze systém, ve kterém je nainstalována příslušná aplikace.

   Pokud potřebujete vyloučit některé pevné disky ze šifrování, vytvořte pro tyto pevné disky seznam.

8. Nakonfigurujte pravidla pro přidávání účtů agenta ověřování během šifrování disku. Agent umožňuje uživateli provést ověření pro přístup k šifrovaným jednotkám a načtení operačního systému. Chcete-li automaticky přidat účty agenta ověřování, nakonfigurujte následující nastavení:

   - **Při šifrování automaticky vytvářet pro uživatele systému Windows účty ověřovacího agenta**. Je-li toto políčko zaškrtnuto, aplikace vytváří účty agenta ověřování na základě seznamu uživatelských účtů Windows v počítači. Ve výchozím nastavení aplikace Kaspersky Endpoint Security používá všechny místní a doménové účty, pomocí kterých se uživatel přihlásil k operačnímu systému za posledních 30 dní.
   - **Vytvářet pro všechny uživatele tohoto počítače účty ověřovacího agenta automaticky při přihlášení**. Je-li toto políčko zaškrtnuto, aplikace před spuštěním ověřovacího agenta zkontroluje informace o uživatelských účtech Windows v počítači. Pokud aplikace Kaspersky Endpoint Security zjistí uživatelský účet systému Windows, který nemá účet ověřovacího agenta, aplikace vytvoří nový účet pro přístup k šifrovaným jednotkám. Nový účet ověřovacího agenta bude mít následující výchozí nastavení: pouze přihlašování chráněné heslem a změna hesla při prvním ověřování. Proto u počítačů s již zašifrovanými jednotkami nemusíte ručně přidávat účty agenta ověřování pomocí úlohy *Správa účtů ověřovacího agenta*.

Pokud jste zakázali automatické vytváření účtů ověřovacího agenta, můžete ručně přidat účty ověřovacího agenta pomocí úlohy *Spravovat účty*. Tuto úlohu můžete také použít ke změně nastavení účtů ověřovacího agenta, které byly vytvořeny automaticky.

9. Pro pohodlí uživatele můžete uživatelské jméno uložit do paměti ověřovacího agenta, aby uživatel musel zadat heslo pouze při příštím přihlášení do systému. Chcete-li tak učinit, zaškrtněte políčko **Uložit uživatelské jméno zadané v ověřovacím agentovi**.

10. Vyberte jeden z následujících způsobů šifrování:

    - Zaškrtněte políčko **Zašifrovat pouze využité místo na disku**, pokud chcete použít šifrování jen na sektory pevného disku, které obsahují soubory.

      Pokud chcete použít šifrování na jednotku, která se již používá, doporučujeme zašifrovat celou jednotku. Zajistíte tím ochranu veškerých dat – i odstraněných dat, která mohou obsahovat čitelné informace. Funkci **Zašifrovat pouze využité místo na disku** doporučujeme používat pro zcela nové jednotky, které nebyly předtím používány.

    - Pokud chcete zašifrovat celý pevný disk, zaškrtnutí políčka **Zašifrovat pouze využité místo na disku** zrušte.

      Pokud bylo nějaké zařízení dříve zašifrováno pomocí funkce **Zašifrovat pouze využité místo na disku**, po použití zásad v režimu **Šifrovat všechny pevné disky** nebudou sektory, v nichž nejsou žádné soubory, zašifrovány.

11. Pokud během šifrování počítače dojde k hardwarové nekompatibilitě, můžete zaškrtnout políčko **Použít funkci Legacy USB Support**.

    Legacy USB Support **je** funkce BIOS/UEFI, která vám umožní používat zařízení USB (například token zabezpečení) během fáze spouštění počítače před spuštěním operačního systému (režim BIOS). Funkce Legacy USB Support neovlivňuje podporu zařízení USB po spuštění operačního systému.

    Je-li funkce Legacy USB Support aktivována, ověřovací agent v režimu BIOS nepodporuje práci s tokeny přes USB. Tuto funkci doporučujeme používat pouze v případě, že dochází k problémům s kompatibilitou hardwaru, a pouze u počítačů, ve kterých k problémům dochází.

12. Uložte změny.

Nástroj Sledování šifrování můžete použít k řízení procesu šifrování nebo dešifrování disku v počítači uživatele. Nástroj Sledování šifrování můžete spustit z hlavního okna aplikace.

Pokud jsou systémové pevné disky zašifrované, před spuštěním operačního systému se načte ověřovací agent. Pomocí ověřovacího agenta dokončete ověření potřebné k získání přístupu k zašifrovaným systémovým pevným diskům a načtení operačního systému. Po úspěšném dokončení postupu ověřování se načte operační systém. Ověření se provádí po každém opětovném spuštění operačního systému.

Vytvoření seznamu pevných disků vyloučených ze šifrování

Seznam výjimek ze šifrování můžete vytvořit jen pro technologii Kaspersky Disk Encryption.

Postup vytvoření seznamu pevných disků vyloučených ze šifrování:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.

6. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **Kaspersky Disk Encryption**.

   Záznamy odpovídající pevným diskům vyloučeným ze šifrování se zobrazí v tabulce **Nešifrovat následující pevné disky**. Tato tabulka bude prázdná, pokud jste předtím nevytvořili žádný seznam pevných disků vyloučených ze šifrování.

7. Postup přidání pevných disků na seznam pevných disků vyloučených ze šifrování:

   a. Klikněte na tlačítko **Přidat**.

      Otevře se okno **Přidat zařízení ze seznamu aplikace Kaspersky Security Center**.

   b. V okně **Přidat zařízení ze seznamu aplikace Kaspersky Security Center** zadejte hodnoty následujících parametrů: **Název**, **Počítač**, **Typ disku**, a **Kaspersky Disk Encryption**.

   c. Klikněte na tlačítko **Aktualizovat**.

   d. Ve sloupci **Název** zaškrtněte políčka na řádcích tabulky odpovídajícím pevným diskům, které chcete přidat na seznam pevných disků vyloučených ze šifrování.

   e. Klikněte na tlačítko **OK**.

   Vybrané pevné disky se zobrazí v tabulce **Nešifrovat následující pevné disky**.

8. Pokud chcete z tabulky výjimek odebrat nějaké pevné disky, vyberte jeden nebo více řádků v tabulce **Nešifrovat následující pevné disky** a klikněte na tlačítko **Odstranit**.

   Více řádků v tabulce můžete vybrat přidržením klávesy **CTRL** a zvolením požadovaných řádků.

9. Uložte změny.

Export a import seznamu pevných disků vyloučených ze šifrování

Seznam výjimek šifrování pevného disku můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství výjimek stejného typu. Funkci exportu/importu můžete také použít k zálohování seznamu výjimek nebo k migraci výjimek na jiný server.

Jak exportovat a importovat seznam výjimek z šifrování pevného disku v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.
6. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **Kaspersky Disk Encryption**.

   Záznamy odpovídající pevným diskům vyloučeným ze šifrování se zobrazí v tabulce **Nešifrovat následující pevné disky**.
7. Postup exportu seznamu výjimek:
   a. Vyberte výjimky, které chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.

      Pokud jste žádnou výjimku nevybrali, aplikace Kaspersky Endpoint Security exportuje všechny výjimky.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
8. Postup importu seznamu pravidel:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
9. Uložte změny.

[Jak exportovat a importovat seznam výjimek z šifrování pevného disku ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam výjimek.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Vyberte možnosti **Šifrování dat** → **Úplné šifrování disku**.
5. Vyberte technologii **Kaspersky Disk Encryption** a po kliknutí na odkaz nakonfigurujte nastavení.

   Otevře se nastavení šifrování.
6. Klikněte na odkaz **Výjimky**.
7. Postup exportu seznamu pravidel:
   a. Vyberte výjimky, které chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrďte, jestli chcete exportovat pouze vybrané výjimky, nebo exportovat celý seznam výjimek.
   d. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.
   e. Klikněte na tlačítko **Uložit**.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
8. Postup importu seznamu pravidel:
   a. Klikněte na tlačítko **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
9. Uložte změny.

Povolení technologie SSO (Single Sign-On)

Technologie SSO (Single Sign-On) umožňuje automatické přihlašování k operačnímu systému pomocí přihlašovacích údajů ověřovacího agenta.

Při použití technologie SSO ignoruje ověřovací agent požadavky na sílu hesla uvedené v aplikaci Kaspersky Security Center. Požadavky na sílu hesla můžete nastavit v nastavení operačního systému.

Technologie SSO není kompatibilní s poskytovateli přihlašovacích údajů třetích stran.

[Jak povolit použití technologie SSO konzole pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Běžné nastavení šifrování**.
6. V bloku **Nastavení hesla** klikněte na tlačítko **Nastavení**.
7. V okně, které se otevře, zaškrtněte na kartě **Ověřovací agent** políčko **Použít technologii SSO (Single Sign-On)**.
8. Uložte změny.

Uživatel tak bude muset ověření provést pouze jednou pomocí agenta. Pro načtení operačního systému není vyžadován proces ověření. Operační systém se načte automaticky.

[Jak povolit použití technologie SSO ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete povolit používání technologie SSO.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Šifrování dat** → **Úplné šifrování disku**.
5. Vyberte technologii **Kaspersky Disk Encryption** a po kliknutí na odkaz nakonfigurujte nastavení.

   Otevře se nastavení šifrování.
6. V části **Nastavení hesla** zaškrtněte políčko **Použít technologii SSO (Single Sign-On)**.
7. Klikněte na tlačítko **OK**.

Uživatel tak bude muset ověření provést pouze jednou pomocí agenta. Pro načtení operačního systému není vyžadován proces ověření. Operační systém se načte automaticky.

Aby technologie SSO fungovala, musí se shodovat heslo účtu systému Windows s heslem pro ověřovacího agenta. Pokud se hesla neshodují, musí uživatel provést ověření dvakrát: v rozhraní ověřovacího agenta a před načtením operačního systému. Poté Kaspersky Endpoint Security nahradí heslo účtu ověřovacího agenta heslem účtu systému Windows.

Správa účtů ověřovacího agenta

Ověřovací agent je potřebný pro práci s jednotkami, které jsou chráněny technologií Kaspersky Disk Encryption (FDE). Před načtením operačního systému musí uživatel dokončit ověření agentem. Úloha *Správa účtů ověřovacího agenta* je navržena pro konfiguraci nastavení ověření uživatele. Můžete použít místní úkoly pro jednotlivé počítače i skupinové úkoly pro počítače ze samostatných skupin správy nebo z výběru počítačů.

Nemůžete nakonfigurovat plán pro spuštění úlohy *Správa účtů ověřovacího agenta*. Je také nemožné násilně zastavit úlohu.

Jak vytvořit úlohu Správa účtů ověřovacího agenta v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Server pro správu** → **Úlohy**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Nová úloha**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnosti **Kaspersky Endpoint Security pro systém Windows (11.6.0)** → **Správa účtů ověřovacího agenta**.

Krok 2. Výběr příkazu pro správu účtu ověřovacího agenta

Vygenerujte seznam příkazů pro správu účtu ověřovacího agenta. Příkazy správy umožňují přidávat, upravovat a odstraňovat účty ověřovacího agenta (viz pokyny níže). Pouze uživatelé, kteří mají účet ověřovacího agenta, mohou dokončit proces ověření, načíst operační systém a získat přístup k šifrované jednotce.

Krok 3. Výběr zařízení, ke kterým bude úloha přiřazena

Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:

- Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
- Vyberte počítače zjištěné serverem pro správu v síti – *nepřiřazená zařízení*. Konkrétní zařízení mohou zahrnovat zařízení ve skupinách pro správu a také nepřiřazená zařízení.
- Zadejte adresy zařízení ručně nebo importujte adresy ze seznamu. Můžete zadat názvy rozhraní NetBIOS, IP adresy a podsítě IP zařízení, ke kterým chcete úlohu přiřadit.

Krok 4. Definování názvu úlohy

Zadejte název úlohy, například `účty správce`.

Krok 5. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Spustit úlohu po dokončení průvodce**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Výsledkem je, že po dokončení úlohy při příštím spuštění počítače může nový uživatel dokončit proceduru ověření, načíst operační systém a získat přístup k šifrované jednotce.

Jak vytvořit úlohu Správa účtů ověřovacího agenta ve webové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Přidat**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Aplikace** vyberte položku **Kaspersky Endpoint Security pro systém Windows (11.6.0)**.
2. V rozevíracím seznamu **Typ úlohy** vyberte možnost **Správa účtů ověřovacího agenta**.
3. Do pole **Název úlohy** zadejte krátký popis, například `Účty správce`.
4. V části **výběru zařízení, ke kterým bude úloha přiřazena** vyberte rozsah úlohy.

Krok 2. Správa účtů ověřovacího agenta

Vygenerujte seznam příkazů pro správu účtu ověřovacího agenta. Příkazy správy umožňují přidávat, upravovat a odstraňovat účty ověřovacího agenta (viz pokyny níže). Pouze uživatelé, kteří mají účet ověřovacího agenta, mohou dokončit proces ověření, načíst operační systém a získat přístup k šifrované jednotce.

Krok 3. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Dokončit** dokončete průvodce. V seznamu úloh se zobrazí nová úloha.

Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**.

Výsledkem je, že po dokončení úlohy při příštím spuštění počítače může nový uživatel dokončit proceduru ověření, načíst operační systém a získat přístup k šifrované jednotce.

Chcete-li přidat účet ověřovacího agenta, musíte do úlohy *Správa účtů ověřovacího agenta* přidat zvláštní příkaz. Je vhodné použít skupinovou úlohu, například přidat účet správce do všech počítačů.

Aplikace Kaspersky Endpoint Security umožňuje automaticky vytvořit účty ověřovacího agenta před šifrováním jednotky. Automatické nastavení účtů ověřovacího agenta můžete povolit v nastavení zásad součásti Úplné šifrování disku. Můžete také použít technologii SSO (Single Sign-On).

Jak přidat účet ověřovacího agenta prostřednictvím konzoly pro správu (MMC)

1. Otevřete vlastnosti úlohy *Správa účtů ověřovacího agenta*.
2. V okně vlastností úlohy vyberte část **Nastavení**.
3. Klikněte na možnosti **Přidat** → **Příkaz přidání účtu**.
4. V okně, které se otevře, zadejte do pole **účtu systému Windows** název účtu systému Microsoft Windows, který bude použit k vytvoření účtu ověřovacího agenta.
5. Pokud jste zadali název účtu Windows ručně, klikněte na tlačítko **Povolit** a určete identifikátor zabezpečení účtu (SID).

   Pokud nebudete chtít SID určit kliknutím na tlačítko **Povolit**, bude určeno při provádění úlohy v počítači.

   > Definování identifikátoru zabezpečení účtu Windows je nutné k ověření správného zadání názvu účtu Windows. Pokud účet Windows neexistuje v počítači nebo v důvěryhodné doméně, skončí úloha *Správa účtů ověřovacího agenta* chybou.

6. Zaškrtněte políčko **Nahradit existující účet**, pokud chcete, aby byl existující účet dříve vytvořený pro ověřovacího agenta nahrazen aktuálně vytvářeným účtem.

   > Tento krok je dostupný, když přidáváte příkaz k vytvoření účtu ověřovacího agenta do vlastností úlohy skupiny pro správu účtů ověřovacího agenta. Tento krok není k dispozici v případě, že přidáte příkaz k vytvoření účtu ověřovacího agenta do vlastností místní úlohy **úplné šifrování disku, správa účtu**.

7. Do pole **Uživatelské jméno** zadejte název účtu ověřovacího agenta, který musí být zadán během ověřování pro přístup k šifrovaným pevným diskům.
8. Zaškrtněte políčko **Povolit ověřování na základě hesla**, pokud chcete, aby aplikace vyzvala uživatele k zadání hesla účtu ověřovacího agenta během ověřování pro přístup k šifrovaným pevným diskům. Nastavte heslo pro účet ověřovacího agenta. V případě potřeby můžete po prvním ověření požádat uživatele o nové heslo.
9. Zaškrtněte políčko **Povolit ověřování na základě certifikátu**, pokud chcete, aby aplikace vyzvala uživatele k připojení tokenu nebo čipové karty k počítači během ověřování pro přístup k šifrovaným pevným diskům. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu.
10. Je-li třeba, zadejte do pole **Popis příkazu** podrobnosti účtu ověřovacího agenta, které potřebujete ke správě příkazu.
11. Proveďte jednu z následujících akcí:

    - Vyberte možnost **Povolit ověření**, pokud chcete, aby aplikace povolila uživateli, který používá účet zadaný v příkazu, přístup k ověřovacímu dialogu ověřovacího agenta.
    - Vyberte možnost **Blokovat ověření**, pokud chcete, aby aplikace neumožnila uživateli, který používá účet zadaný v příkazu, přístup k ověřovacímu dialogu ověřovacího agenta.

12. Uložte změny.

[Jak přidat účet ověřovacího agenta prostřednictvím webové konzoly]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Správa účtů ověřovacího agenta** aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Nastavení aplikace**.

4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Přidat**.

   Spustí se průvodce správou účtů ověřovacího agenta.

5. Vyberte typ příkazu **Přidat účet**.

6. Vyberte uživatelský účet. Účet můžete vybrat ze seznamu doménových účtů nebo ručně zadat název účtu. Klikněte na tlačítko **Další**.

   Kaspersky Endpoint Security určuje identifikátor zabezpečení účtu (SID). To je nutné k ověření účtu. Pokud jste zadali uživatelské jméno nesprávně, aplikace Kaspersky Endpoint Security úlohu ukončí s chybou.

7. Nakonfigurujte nastavení účtu ověřovacího agenta.

   - **Vytvořte nový účet ověřovacího agenta, kterým nahradíte stávající účet**. Aplikace Kaspersky Endpoint Security prohledává stávající účty v počítači. Pokud se ID zabezpečení uživatele v počítači a v úloze shoduje, Kaspersky Endpoint Security změní nastavení účtu v souladu s úlohou.

   - **Uživatelské jméno**. Výchozí uživatelské jméno účtu ověřovacího agenta se shoduje názvu domény uživatele.

   - **Povolit ověřování na základě hesla**. Nastavte heslo pro účet ověřovacího agenta. V případě potřeby můžete po prvním ověření požádat uživatele o nové heslo. Pokud zvolíte tuto možnost, bude mít každý uživatel své vlastní jedinečné heslo. V zásadách můžete také nastavit požadavky na sílu hesla pro účet ověřovacího agenta.

   - **Povolit ověřování na základě certifikátu**. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu. Uživatel tak bude muset zadat heslo pro čipovou kartu nebo token.

   - **Přístup účtu k šifrovaným datům**. Zde můžete nakonfigurovat přístup uživatele k šifrované jednotce. Můžete například namísto odstranění účtu ověřovacího agenta dočasně zakázat ověřování uživatelů.

   - **Poznámka**. V případě potřeby zadejte popis účtu.

8. Uložte změny.

9. Zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Spustit**.

   Výsledkem je, že po dokončení úlohy při příštím spuštění počítače může nový uživatel dokončit proceduru ověření, načíst operační systém a získat přístup k šifrované jednotce.

Chcete-li změnit heslo a další nastavení ověřovacího agenta, musíte do úlohy *Správa účtů ověřovacího agenta* přidat zvláštní příkaz. Je vhodné použít skupinovou úlohu, například nahradit certifikát tokenu správce na všech počítačích.

[Jak změnit účet ověřovacího agenta prostřednictvím konzoly pro správu (MMC)]

1. Otevřete vlastnosti úlohy *Správa účtů ověřovacího agenta*.
2. V okně vlastností úlohy vyberte část **Nastavení**.
3. Klikněte na možnosti **Přidat** → **Příkaz úprav účtu**.
4. V okně, které se otevře, zadejte do pole **účtu systému Windows** název uživatelského účtu systému Microsoft Windows, který chcete změnit.
5. Pokud jste zadali název účtu Windows ručně, klikněte na tlačítko **Povolit** a určete identifikátor zabezpečení účtu (SID).

   Pokud nebudete chtít SID určit kliknutím na tlačítko **Povolit**, bude určeno při provádění úlohy v počítači.

   > Definování identifikátoru zabezpečení účtu Windows je nutné k ověření správného zadání názvu účtu Windows. Pokud účet Windows neexistuje v počítači nebo v důvěryhodné doméně, skončí úloha *Správa účtů ověřovacího agenta* chybou.

6. Zaškrtněte políčko **Změnit uživatelské jméno** a zadejte nový název účtu ověřovacího agenta, pokud chcete, aby aplikace Kaspersky Endpoint Security změnila uživatelské jméno pro všechny účty ověřovacího agenta vytvořené pomocí účtu systému Microsoft Windows s názvem uvedeným v poli **Účet systému Windows** na jméno zadané do pole níže.
7. Zaškrtněte políčko **Změnit nastavení ověření na základě hesla**, pokud chcete, aby bylo možné upravit nastavení ověření pomocí hesla.
8. Zaškrtněte políčko **Povolit ověřování na základě hesla**, pokud chcete, aby aplikace vyzvala uživatele k zadání hesla účtu ověřovacího agenta během ověřování pro přístup k šifrovaným pevným diskům. Nastavte heslo pro účet ověřovacího agenta.
9. Zaškrtněte políčko **Upravit pravidlo změny hesla při ověření v ověřovacím agentovi**, pokud chcete, aby aplikace Kaspersky Endpoint Security změnila hodnotu nastavení změny hesla pro všechny účty ověřovacího agenta vytvořené pomocí účtu systému Microsoft Windows s názvem uvedeným v poli **Účet systému Windows** na hodnotu nastavení zadanou níže.
10. Zadejte hodnotu nastavení změny hesla při ověřování v rámci ověřovacího agenta.
11. Zaškrtněte políčko **Změnit nastavení ověření na základě certifikátu**, pokud chcete, aby bylo možné upravit nastavení ověření na základě elektronického certifikátu tokenu nebo čipové karty.
12. Zaškrtněte políčko **Povolit ověřování na základě certifikátu**, pokud chcete, aby aplikace vyzvala uživatele k zadání hesla tokenu nebo čipové karty připojené k počítači během ověřování pro přístup k šifrovaným pevným diskům. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu.
13. Zaškrtněte políčko **Upravit popis příkazu** a upravte popis příkazu, pokud chcete, aby aplikace Kaspersky Endpoint Security změnila popis příkazu pro všechny účty ověřovacího agenta vytvořené pomocí účtu systému Microsoft Windows s názvem uvedeným v poli **Účet systému Windows**.
14. Zaškrtněte políčko **Upravit pravidlo přístupu k ověření v ověřovacím agentovi**, pokud chcete, aby aplikace Kaspersky Endpoint Security změnila pravidlo pro přístup uživatele k ověřovacímu dialogu ověřovacího agenta na hodnotu zadanou níže pro všechny účty ověřovacího agenta vytvořené pomocí účtu systému Microsoft Windows s názvem uvedeným v poli **Účet systému Windows**.
15. Zadejte pravidlo přístupu k ověřovacímu dialogu v rámci ověřovacího agenta.

16. Uložte změny.

[Jak změnit účet ověřovacího agenta prostřednictvím webové konzoly]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Správa účtů ověřovacího agenta** aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Nastavení aplikace**.

4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Přidat**.

   Spustí se průvodce správou účtů ověřovacího agenta.

5. Vyberte typ příkazu **Upravit účet**.

6. Vyberte uživatelský účet. Účet můžete vybrat ze seznamu doménových účtů nebo ručně zadat název účtu. Klikněte na tlačítko **Další**.

   Kaspersky Endpoint Security určuje identifikátor zabezpečení účtu (SID). To je nutné k ověření účtu. Pokud jste zadali uživatelské jméno nesprávně, aplikace Kaspersky Endpoint Security úlohu ukončí s chybou.

7. Zaškrtněte políčka vedle nastavení, která chcete upravit.

8. Nakonfigurujte nastavení účtu ověřovacího agenta.

   - **Vytvořte nový účet ověřovacího agenta, kterým nahradíte stávající účet**. Aplikace Kaspersky Endpoint Security prohledává stávající účty v počítači. Pokud se ID zabezpečení uživatele v počítači a v úloze shoduje, Kaspersky Endpoint Security změní nastavení účtu v souladu s úlohou.

   - **Uživatelské jméno**. Výchozí uživatelské jméno účtu ověřovacího agenta se shoduje názvu domény uživatele.

   - **Povolit ověřování na základě hesla**. Nastavte heslo pro účet ověřovacího agenta. V případě potřeby můžete po prvním ověření požádat uživatele o nové heslo. Pokud zvolíte tuto možnost, bude mít každý uživatel své vlastní jedinečné heslo. V zásadách můžete také nastavit požadavky na sílu hesla pro účet ověřovacího agenta.

   - **Povolit ověřování na základě certifikátu**. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu. Uživatel tak bude muset zadat heslo pro čipovou kartu nebo token.

   - **Přístup účtu k šifrovaným datům**. Zde můžete nakonfigurovat přístup uživatele k šifrované jednotce. Můžete například namísto odstranění účtu ověřovacího agenta dočasně zakázat ověřování uživatelů.

   - **Poznámka**. V případě potřeby zadejte popis účtu.

9. Uložte změny.

10. Zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Spustit**.

Chcete-li odstranit účet ověřovacího agenta, musíte do úlohy *Správa účtů ověřovacího agenta* přidat zvláštní příkaz. Je vhodné použít skupinovou úlohu, například odstranit účet propuštěného zaměstnance.

[Jak odstranit účet ověřovacího agenta prostřednictvím konzoly pro správu (MMC)]

1. Otevřete vlastnosti úlohy *Správa účtů ověřovacího agenta*.
2. V okně vlastností úlohy vyberte část **Nastavení**.
3. Klikněte na možnosti **Přidat** → **Příkaz odstranění účtu**.
4. V okně, které se otevře, do pole **účtu systému Windows** zadejte název uživatelského účtu systému Microsoft Windows použitého k vytvoření účtu ověřovacího agenta, který chcete odstranit.
5. Pokud jste zadali název účtu Windows ručně, klikněte na tlačítko **Povolit** a určete identifikátor zabezpečení účtu (SID).

   Pokud nebudete chtít SID určit kliknutím na tlačítko **Povolit**, bude určeno při provádění úlohy v počítači.

   > Definování identifikátoru zabezpečení účtu Windows je nutné k ověření správného zadání názvu účtu Windows. Pokud účet Windows neexistuje v počítači nebo v důvěryhodné doméně, skončí úloha *Správa účtů ověřovacího agenta* chybou.

6. Uložte změny.

[Jak odstranit účet ověřovacího agenta prostřednictvím webové konzoly]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Správa účtů ověřovacího agenta** aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Nastavení aplikace**.
4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Přidat**.

   Spustí se průvodce správou účtů ověřovacího agenta.
5. Vyberte typ příkazu **Odstranit účet**.
6. Vyberte uživatelský účet. Účet můžete vybrat ze seznamu doménových účtů nebo ručně zadat název účtu.
7. Uložte změny.
8. Zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Spustit**.

   Výsledkem je, že po dokončení úlohy při příštím spuštění počítače nebude uživatel schopen dokončit proceduru ověření a načíst operační systém. Aplikace Kaspersky Endpoint Security zakáže přístup k šifrovaným datům.

Chcete-li zobrazit seznam uživatelů, kteří mohou dokončit ověřování pomocí agenta a načíst operační systém, musíte přejít do vlastností spravovaného počítače.

[Jak zobrazit seznam účtů ověřovacího agenta prostřednictvím konzoly pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Dvojitým kliknutím otevřete okno vlastností počítače.
5. V okně vlastností počítače vyberte část **Úlohy**.

   Otevře se seznam místních úloh.
6. Vyberte úlohu **Správa účtů ověřovacího agenta**.
7. V okně vlastností úlohy vyberte část **Nastavení**.

Díky tomu budete mít přístup k seznamu účtů ověřovacího agenta v tomto počítači. Pouze uživatelé ze seznamu mohou dokončit ověřování pomocí agenta a načíst operační systém.

[Jak zobrazit seznam účtů ověřovacího agenta prostřednictvím webové konzoly]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Klikněte na název počítače, na kterém chcete zobrazit seznam účtů ověřovacího agenta.

   Otevřou se vlastnosti počítače.
3. V okně vlastností počítače vyberte část **Úlohy**.

   Otevře se seznam místních úloh.
4. Vyberte úlohu **Správa účtů ověřovacího agenta**.
5. Ve vlastnostech úlohy vyberte část **Nastavení aplikace**.

Díky tomu budete mít přístup k seznamu účtů ověřovacího agenta v tomto počítači. Pouze uživatelé ze seznamu mohou dokončit ověřování pomocí agenta a načíst operační systém.

Použití tokenu a čipové karty v kombinaci s ověřovacím agentem

Token nebo čipovou kartu lze použít k ověření pro přístup k šifrovaným pevným diskům. Chcete-li tak učinit, musíte do úlohy *Správa účtů ověřovacího agenta* přidat elektronický soubor certifikátů tokenu nebo čipové karty.

Použití tokenu nebo čipové karty bude k dispozici, pouze pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES256. Pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES56, přiřazení souboru elektronického certifikátu k příkazu bude zamítnuto.

Aplikace Kaspersky Endpoint Security podporuje následující tokeny, čtečky čipových karet a čipové karty:

- SafeNet eToken PRO 64K (4.2b)
- SafeNet eToken PRO 72K Java
- SafeNet eToken 4100-72K (Java)
- SafeNet eToken 5100
- SafeNet eToken 5105
- SafeNet eToken 7300
- EMC RSA SID 800
- Gemalto IDPrime.NET 510
- Gemalto IDPrime.NET 511
- Rutoken ECP
- Rutoken ECP Flash
- Aladdin-RD JaCarta PKI
- Athena IDProtect Laser
- SafeNet eToken PRO 72K Java
- Aladdin-RD JaCarta PKI

Chcete-li přiřadit soubor elektronického certifikátu tokenu nebo čipové karty k příkazu pro vytvoření účtu ověřovacího agenta, musíte nejprve uložit soubor pomocí externího softwaru pro správu certifikátů.

Certifikát tokenu nebo čipové karty musí mít následující vlastnosti:

- Certifikát musí být v souladu se standardem X.509 a soubor certifikátu musí mít kódování DER.
- Certifikát obsahuje klíč RSA s délkou alespoň 1024 bitů.

Pokud elektronický certifikát tokenu nebo čipové karty nesplňuje tyto požadavky, nemůžete načíst soubor certifikátu do příkazu pro vytvoření účtu ověřovacího agenta.

Parametr `KeyUsage` musí mít hodnotu `keyEncipherment` nebo `dataEncipherment`. Parametr `KeyUsage` určuje účel certifikátu. Pokud má parametr jinou hodnotu, Kaspersky Security Center stáhne soubor certifikátu, ale zobrazí varování.

Pokud uživatel ztratil token nebo čipovou kartu, správce musí přiřadit soubor elektronického certifikátu tokenu nebo čipové karty k příkazu pro vytvoření účtu ověřovacího agenta. Poté musí uživatel dokončit postup získání přístupu k zašifrovaným zařízením nebo obnovení dat v zašifrovaných zařízeních.

Dešifrování pevných disků

Pevné disky můžete dešifrovat, i když není k dispozici žádná aktivní licence povolující šifrování dat.

Postup dešifrování pevných disků:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.
6. V rozevíracím seznamu **Technologie šifrování** vyberte technologii, pomocí které byly pevné disky šifrovány.
7. Proveďte jednu z následujících akcí:
   - V rozevíracím seznamu **Režim šifrování** vyberte možnost **Dešifrovat všechny pevné disky**, chcete-li dešifrovat všechny šifrované pevné disky.
   - Šifrované pevné disky, které chcete dešifrovat, přidejte do tabulky **Nešifrovat následující pevné disky**.

     Tato možnost je dostupná jen pro technologii Kaspersky Disk Encryption.
8. Uložte změny.

Nástroj Sledování šifrování můžete použít k řízení procesu šifrování nebo dešifrování disku v počítači uživatele. Nástroj Sledování šifrování můžete spustit z hlavního okna aplikace.

Jestliže uživatel vypne nebo restartuje počítač během dešifrování pevných disků zašifrovaných pomocí technologie Kaspersky Disk Encryption, před příštím spuštěním operačního systému se načte ověřovací agent. Po úspěšném ověření pomocí ověřovacího agenta a spuštění operačního systému obnoví aplikace Kaspersky Endpoint Security dešifrování pevného disku.

Jestliže se během šifrování pevných disků zašifrovaných pomocí technologie Kaspersky Disk Encryption přepne operační systém do režimu hibernace, po ukončení režimu hibernace se načte ověřovací agent. Po úspěšném ověření pomocí ověřovacího agenta a spuštění operačního systému obnoví aplikace Kaspersky Endpoint Security dešifrování pevného disku. Po dešifrování pevného disku nebude režim hibernace dostupný, dokud nebude proveden první restart operačního systému.

Jestliže během dešifrování pevného disku přejde operační systém do režimu spánku, aplikace Kaspersky Endpoint Security obnoví dešifrování pevného disku, jakmile dojde k ukončení režimu spánku (ověřovací agent se nenačte).

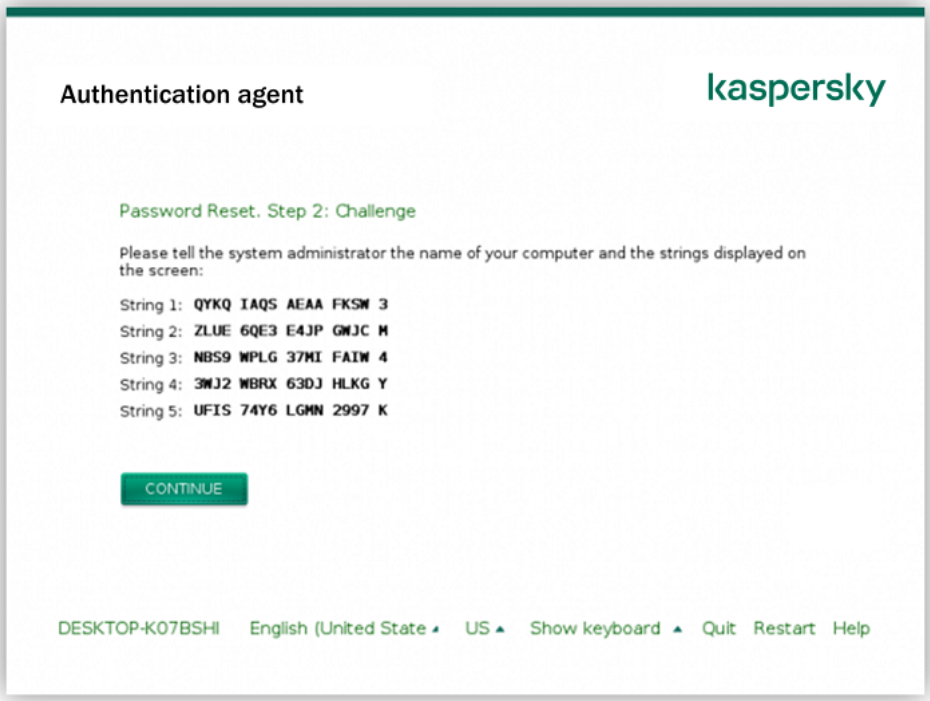
Obnovení přístupu k jednotce chráněné technologií Kaspersky Disk Encryption

Pokud uživatel zapomněl heslo pro přístup k pevnému disku chráněnému technologií Kaspersky Disk Encryption, musí zahájit proces obnovení (žádost–odpověď).

Obnovení přístupu k systémovému pevnému disku

Obnovení přístupu k systémovému pevnému disku chráněnému technologií Kaspersky Disk Encryption se skládá z následujících kroků:

1. Uživatel sdělí bloky žádosti správci (viz obrázek níže).
2. Správce zadá bloky žádosti do aplikace Kaspersky Security Center, obdrží bloky odpovědí a sdělí je uživateli.
3. Uživatel zadá bloky odpovědi v rozhraní ověřovacího agenta a získá přístup k pevnému disku.



Obnovení přístupu k systémovému pevnému disku chráněnému technologií Kaspersky Disk Encryption

Chce-li uživatel zahájit proces obnovení, musí v rozhraní ověřovacího agenta kliknout na tlačítko **Zapomenuté heslo**.

[Jak získat bloky odpovědi pro systémový pevný disk chráněný technologií Kaspersky Disk Encryption v konzole pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
5. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
6. V otevřeném okně vyberte kartu **Ověřovací agent**.
7. V části **Používaný šifrovací algoritmus** vyberte šifrovací algoritmus: **AES56** nebo **AES256**.

   Algoritmus šifrování dat závisí na šifrovací knihovně AES, která je součástí distribučního balíčku: *silné šifrování (AES256)* nebo *lehké šifrování (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.
8. V rozevíracím seznamu **Účet** vyberte název účtu ověřovacího agenta vytvořeného pro uživatele, který požaduje obnovení přístupu k disku.
9. V rozevíracím seznamu **Pevný disk** vyberte šifrovaný pevný disk, u kterého potřebujete obnovit přístup.
10. V části **Žádost uživatele** zadejte bloky žádosti nadiktované uživatelem.

    Obsah bloků odpovědi na žádost uživatele o obnovení uživatelského jména a hesla účtu ověřovacího agenta se zobrazí v poli **Přístupový klíč**. Uživateli sdělte obsah bloků odpovědi.

[Jak získat bloky odpovědi pro systémový pevný disk chráněný technologií Kaspersky Disk Encryption ve webové konzole]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.
4. V otevřeném okně vyberte část **Ověřovací agent**.
5. V rozevíracím seznamu **Účet** vyberte název účtu ověřovacího agenta vytvořeného pro uživatele, který požaduje obnovení uživatelského jména a hesla účtu ověřovacího agenta.
6. Zadejte bloky žádosti sdělené uživatelem.

   Obsah bloků odpovědi na žádost uživatele o obnovení uživatelského jména a hesla účtu ověřovacího agenta se zobrazí v dolní části okna. Uživateli sdělte obsah bloků odpovědi.

Po dokončení procesu obnovení vyzve ověřovací agent uživatele, aby změnil heslo.

Obnovení přístupu k nesystémovému pevnému disku

Obnovení přístupu k nesystémovému pevnému disku chráněnému technologií Kaspersky Disk Encryption se skládá z následujících kroků:

1. Uživatel odešle správci soubor se žádostí o přístup.
2. Správce přidá soubor se žádostí o přístup do aplikace Kaspersky Security Center, vytvoří soubor přístupového klíče a odešle jej uživateli.
3. Uživatel přidá soubor klíče přístupu do aplikace Kaspersky Endpoint Security a získá přístup k souborům.

Chce-li uživatel zahájit proces obnovení, musí se pokusit o přístup k pevnému disku. Aplikace Kaspersky Endpoint Security pak vytvoří soubor se žádostí o přístup (soubor s příponou KESDC), který uživatel musí zaslat správci, například e-mailem.

Jak získat soubor přístupového klíče pro šifrovaný nesystémový pevný disk v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
5. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
6. V otevřeném okně vyberte kartu **Šifrování dat**.
7. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.
8. V okně pro výběr souboru se žádostí o přístup zadejte cestu k souboru přijatému od uživatele.

   Zobrazí se informace o požadavku uživatele. Aplikace Kaspersky Security Center vygeneruje soubor klíče. Vygenerovaný soubor klíče šifrovaného přístupu k datům zašlete uživateli e-mailem. Případně přístupový soubor uložte a k přenosu souboru použijte libovolnou dostupnou metodu.

Jak získat soubor klíče šifrovaného přístupu k nesystémovému pevnému disku ve webové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.
4. Vyberte část **Šifrování dat**.
5. Klikněte na tlačítko **Vybrat soubor** a vyberte soubor se žádostí o přístup, který jste obdrželi od uživatele (soubor s příponou KESDC).

   Ve webové konzole se zobrazí informace o požadavku. Ty budou zahrnovat název počítače, na kterém uživatel požaduje přístup k souboru.
6. Klikněte na tlačítko **Uložit klíč** a vyberte složku, do které chcete uložit soubor klíče šifrovaného přístupu k datům (soubor s příponou KESDR).

Díky tomu budete moci získat soubor klíče šifrovaného přístupu k datům, který budete musíte předat uživateli.

Aktualizace operačního systému

Při aktualizaci operačního systému počítače, který je chráněn šifrováním na úrovni souborů (FDE), je nutné brát v úvahu zvláštní faktory. Operační systém aktualizuje následujícím způsobem: nejprve aktualizujte OS na jednom počítači, poté aktualizujte OS na malé části počítačů a poté aktualizujte OS na všech počítačích v síti.

Pokud používáte technologii Kaspersky Disk Encryption, spuštěním operačního systému se načte ověřovací agent. Pomocí ověřovacího agenta se uživatel může přihlásit do systému a získat přístup k šifrovaným jednotkám. Poté se začne načítat operační systém.

Pokud spustíte aktualizaci operačního systému v počítači, který je chráněn pomocí technologie Kaspersky Disk Encryption, průvodce aktualizací OS agenta ověřování odebere. V důsledku toho může být počítač uzamčen, protože zavaděč OS nebude mít přístup k šifrované jednotce.

Podrobnosti o bezpečné aktualizaci operačního systému najdete ve znalostní bázi technické podpory.

Automatická aktualizace operačního systému je k dispozici za následujících podmínek:

1. Operační systém je aktualizován prostřednictvím služby WSUS (Windows Server Update Services).
2. V počítači je nainstalován systém Windows 10 verze 1607 (RS1) nebo novější.
3. V počítači je nainstalována aplikace Kaspersky Endpoint Security verze 11.2.0 nebo novější.

Pokud jsou splněny všechny podmínky, můžete operační systém aktualizovat obvyklým způsobem.

Pokud používáte technologii Kaspersky Disk Encryption (FDE) a v počítači je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows verze 11.1.0 nebo 11.1.1, nemusíte před aktualizací systému Windows 10 dešifrovat pevné disky.

Chcete-li aktualizovat operační systém, musíte provést následující:

1. Před aktualizací systému zkopírujte ovladače s názvem cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf a klfdefsf.sys do místní složky. Například: C:\ovladace_fce.

2. Pomocí přepínače `/ ReflectDrivers` spusťte instalaci aktualizace systému a určete složku obsahující uložené ovladače:

   ```
   setup.exe /ReflectDrivers C:\fde_drivers
   ```

Jestliže používáte technologii BitLocker Drive Encryption, nemusíte pro aktualizaci systému Windows 10 pevné disky dešifrovat. Podrobnější informace o fungování nástroje BitLocker najdete na *webu společnosti Microsoft*.

Odstranění chyb aktualizace funkce šifrování

Funkce Úplné šifrování disku je aktualizována v případě, že předchozí verze aplikace je upgradována na verzi Kaspersky Endpoint Security pro systém Windows 11.6.0.

Při spuštění aktualizace funkce Úplné šifrování disku může dojít k následujícím chybám:

- Nelze inicializovat aktualizaci.
- Zařízení není kompatibilní s ověřovacím agentem.

Postup odstranění chyb, ke kterým došlo při spuštění procesu aktualizace funkce Úplné šifrování disku v nové verzi aplikace:

1. Dešifrujte pevné disky.
2. Znovu zašifrujte pevné disky.

Během aktualizace funkce Úplné šifrování disku může dojít k následujícím chybám:

- Nelze dokončit aktualizaci.
- Vrácení zpět upgradu funkce Úplné šifrování disku je dokončeno s chybou.

Chcete-li odstranit chyby, ke kterým došlo během procesu aktualizace funkce Úplné šifrování disku,

obnovte přístup k šifrovaným zařízením pomocí nástroje pro obnovení.

Výběr úrovně trasování ověřovacího agenta

Aplikace do souboru trasování protokoluje informace o provozu a uživatelském využití ověřovacího agenta.

Postup výběru úrovně trasování ověřovacího agenta:

1. Ihned po zapnutí počítače se šifrovanými pevnými disky vyvolejte stisknutím klávesy **F3** okno ke konfiguraci nastavení ověřovacího agenta.
2. Vyberte úroveň trasování v okně nastavení ověřovacího agenta:
   - **Zakázat protokolování ladění (výchozí)**. Pokud je zvolena tato možnost, aplikace do souboru trasování neprotokoluje informace o událostech ověřovacího agenta.

- **Povolit protokolování ladění**. Pokud je zvolena tato možnost, aplikace do souboru trasování protokoluje informace o provozu a uživatelském využití ověřovacího agenta.
- **Povolit podrobné protokolování**. Pokud je zvolena tato možnost, aplikace do souboru trasování protokoluje podrobné informace o provozu a uživatelském využití ověřovacího agenta.

  Úroveň podrobnosti záznamů při použití této možnosti je vyšší ve srovnání s úrovní možnosti **Povolit protokolování ladění**. Vyšší úroveň podrobnosti záznamů může zpomalit spouštění ověřovacího agenta a operačního systému.

- **Povolit protokolování ladění a zvolit sériový port**. Pokud je zvolena tato možnost, aplikace do souboru trasování protokoluje informace o provozu a uživatelském využití ověřovacího agenta. Tyto informace poté předá prostřednictvím portu COM.

  Pokud je počítač se šifrovanými pevnými disky připojen k jinému počítači prostřednictvím portu COM, události ověřovacího agenta lze prohlížet i prostřednictvím tohoto druhého počítače.

- **Povolit podrobné protokolování a zvolit sériový port**. Pokud je zvolena tato možnost, aplikace do souboru trasování protokoluje podrobné informace o provozu a uživatelském využití ověřovacího agenta. Tyto informace poté předá prostřednictvím portu COM.

  Úroveň podrobnosti záznamů při použití této možnosti je vyšší ve srovnání s úrovní možnosti **Povolit protokolování ladění a zvolit sériový port**. Vyšší úroveň podrobnosti záznamů může zpomalit spouštění ověřovacího agenta a operačního systému.

Data jsou zaznamenávána do souboru trasování ověřovacího agenta, pokud jsou v počítači přítomny šifrované pevné disky nebo během úplného šifrování disku.

Na rozdíl od jiných souborů trasování aplikace není soubor trasování ověřovacího agenta odesílán společnosti Kaspersky. Pokud je to nezbytné, můžete soubor trasování ověřovacího agenta ručně odeslat společnosti Kaspersky za účelem analýzy.

Úprava textů nápovědy pro ověřovacího agenta

Před úpravou zpráv nápovědy pro ověřovacího agenta se podívejte na seznam podporovaných znaků v prostředí před spuštěním (viz níže).

Postup úpravy zpráv nápovědy pro ověřovacího agenta:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat → Běžné nastavení šifrování**.
6. V části **Templates** klikněte na tlačítko **Help**.

Otevře se okno **Authentication Agent help messages**.

7. Postupujte následovně:

   - Vyberte kartu **Authentication** a upravte text nápovědy zobrazující se v okně ověřovacího agenta během zadávání přihlašovacích údajů účtu.
   - Vyberte kartu **Change password** a upravte text nápovědy zobrazující se v okně ověřovacího agenta při změně hesla pro účet ověřovacího agenta.
   - Vyberte kartu **Recover password** a upravte text nápovědy zobrazující se v okně ověřovacího agenta při obnovování hesla pro účet ověřovacího agenta.

8. Upravte zprávy nápovědy.

   Pokud chcete obnovit původní text, klikněte na tlačítko **Výchozí režim**.

   > Můžete zadat text nápovědy obsahující maximálně 16 řádků. Délka každého řádku může být maximálně 64 znaků.

9. Uložte změny.

Omezená podpora znaků ve zprávách nápovědy pro ověřovacího agenta

V prostředí před spuštěním jsou podporovány následující znaky formátu Unicode:

- Základní latinská abeceda (0000–007F)
- Doplňkové znaky Latin-1 (0080–00FF)
- Rozšířená latinka A (0100–017F)
- Rozšířená latinka B (0180–024F)
- Nekombinované znaky s rozšířeným ID (02B0–02FF)
- Kombinované diakritické značky (0300–036F)
- Řecká a koptská abeceda (0370–03FF)
- Cyrilice (0400–04FF)
- Hebrejština (0590–05FF)
- Arabština (0600–06FF)
- Doplňková rozšířená latinka (1E00–1EFF)
- Interpunkční znaménka (2000–206F)
- Symboly měn (20A0–20CF)
- Znaky podobné písmenům (2100–214F)

- Geometrické tvary (25A0–25FF)
- Arabské prezentační formy B (FE70–FEFF)

Znaky, které nejsou v tomto seznamu uvedeny, nejsou v prostředí před spuštěním podporovány. Ve zprávách nápovědy ověřovacího agenta nedoporučujeme takovéto znaky používat.

Odstranění zbylých objektů a dat po testování činnosti ověřovacího agenta

Pokud aplikace Kaspersky Endpoint Security během odinstalace objeví objekty a data, které zůstaly na systémovém pevném disku po testovacím provozu ověřovacího agenta, odinstalace aplikace bude přerušena a nebude možná, dokud tyto objekty a data nebudou odstraněny.

Objekty a data mohou zůstat na systémovém pevném disku po testovacím provozu ověřovacího agenta pouze ve výjimečných případech. To se může stát například v případě, že počítač nebyl restartován po použití zásady aplikace Kaspersky Security Center s nastavením šifrování nebo že se aplikace nespustí po testovacím provozu ověřovacího agenta.

Objekty a data, které na systémovém pevném disku zůstaly po testovacím provozu ověřovacího agenta, můžete odstranit následujícími způsoby:

- pomocí zásad aplikace Kaspersky Security Center;
- pomocí nástroje pro obnovení.

Použití zásad aplikace Kaspersky Security Center k odstranění objektů a dat, které zbyly po testovacím provozu ověřovacího agenta:

1. Použijte na počítač zásady aplikace Kaspersky Security Center s nastavením pro dešifrování všech pevných disků počítače.
2. Spusťte aplikaci Kaspersky Endpoint Security.

Chcete-li odstranit informace o nekompatibilitě aplikací s ověřovacím agentem,

zadejte do příkazového řádku příkaz `avp pbatestreset`.

BitLocker Management

BitLocker je šifrovací technologie zabudovaná do operačních systémů Windows. Aplikace Kaspersky Endpoint Security vám umožňuje řídit a spravovat technologii Bitlocker pomocí aplikace Kaspersky Security Center. BitLocker šifruje logické svazky. BitLocker nelze použít pro šifrování vyměnitelných jednotek. Podrobnosti o technologii BitLocker najdete v dokumentaci společnosti Microsoft.

BitLocker poskytuje zabezpečené úložiště přístupových klíčů pomocí modulu TPM (Trusted Platform Module). *Trusted Platform Module (TPM)* je mikročip vyvinutý pro poskytování základních funkcí souvisejících se zabezpečením (například k ukládání šifrovacích klíčů). Modul TPM je obvykle nainstalován na základní desce počítače a komunikuje se všemi ostatními součástmi systému prostřednictvím hardwarové sběrnice. Použití modulu TPM je nejbezpečnějším způsobem uložení přístupových klíčů nástroje BitLocker, protože modul poskytuje ověření integrity systému před spuštěním. Jednotky v počítači můžete šifrovat i bez modulu TPM. V tomto případě bude přístupový klíč zašifrován pomocí hesla. BitLocker používá následující metody ověřování:

- TPM.

- TPM a PIN.
- Heslo.

Po zašifrování jednotky vytvoří nástroj BitLocker hlavní klíč. Aplikace Kaspersky Endpoint Security odešle hlavní klíč do aplikace Kaspersky Security Center, abyste mohli obnovit přístup na disk, například pokud uživatel zapomene heslo.

Pokud uživatel zašifruje disk pomocí nástroje BitLocker, Kaspersky Endpoint Security pošle informace o šifrování disku do aplikace Kaspersky Security Center. Kaspersky Endpoint Security nicméně do aplikace Kaspersky Security Center neposílá hlavní klíč, takže nebude možné obnovit přístup na disk pomocí aplikace Kaspersky Security Center. Aby nástroj BitLocker správně fungoval s aplikací Kaspersky Security Center, dešifrujte jednotku a znovu ji zašifrujte pomocí zásady. Jednotku můžete dešifrovat místně nebo pomocí zásady.

Po zašifrování systémového pevného disku musí uživatel před spuštěním operačního systému projít ověřením nástrojem BitLocker. Po ověření umožní nástroj BitLocker uživatelům přihlášení. BitLocker nepodporuje technologii jednotného přihlašování (SSO).

Pokud používáte zásady skupiny systému Windows, vypněte správu nástroje BitLocker v nastavení zásad. Nastavení zásad systému Windows může být v rozporu s nastavením zásad aplikace Kaspersky Endpoint Security. Při šifrování jednotky mohou nastat chyby.

Spuštění nástroje BitLocker Drive Encryption

Před spuštěním úplného šifrování disku se doporučuje ověřit, že počítač není infikovaný. To můžete provést spuštěním úlohy Úplná kontrola nebo Kontrola kritických oblastí. Provedení úplného šifrování disku v počítači, který je infikovaný rootkitem, může způsobit nefunkčnost počítače.

Chcete-li používat součást BitLocker Drive Encryption v počítačích s operačními systémy Windows pro servery, může být vyžadována instalace této součásti. Součást nainstalujte pomocí nástrojů operačního systému (průvodce přidáním rolí a součástí). Další informace o instalaci součásti BitLocker Drive Encryption naleznete v dokumentaci společnosti Microsoft.

Jak spustit BitLocker Drive Encryption pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.
6. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **BitLocker Drive Encryption**.
7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Šifrovat všechny pevné disky**.

   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém bylo provedeno šifrování.

8. Nakonfigurujte rozšířené možnosti součásti BitLocker Drive Encryption (viz tabulka níže).
9. Uložte změny.

Jak spustit BitLocker Drive Encryption prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. U počítačů, u nichž chcete spustit BitLocker Drive Encryption, klikněte na název zásady aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Šifrování dat** → **Úplné šifrování disku**.
5. V části **Správa šifrování** vyberte možnost **BitLocker Drive Encryption**.
6. Klikněte na odkaz **BitLocker Drive Encryption**.

   Otevře se okno s nastavením součásti BitLocker Drive Encryption.
7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Šifrovat všechny pevné disky**.

   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém bylo provedeno šifrování.

8. Nakonfigurujte rozšířené možnosti součásti BitLocker Drive Encryption (viz tabulka níže).
9. Klikněte na tlačítko **OK**.

Nástroj Sledování šifrování můžete použít k řízení procesu šifrování nebo dešifrování disku v počítači uživatele. Nástroj Sledování šifrování můžete spustit z hlavního okna aplikace.

Po uplatnění zásady zobrazí aplikace v závislosti na nastavení ověřování tyto dotazy:

- Pouze TPM. Není požadován žádný vstup od uživatele. Disk bude zašifrován při opětovném spuštění počítače.
- TPM + PIN/heslo. Pokud je k dispozici modul TPM, zobrazí se okno s výzvou k zadání kódu PIN. Pokud modul TPM k dispozici není, pro ověření před spuštěním se zobrazí okno s výzvou k zadání hesla.
- Pouze heslo. Uvidíte okno s výzvou k zadání hesla pro ověření před spuštěním.

Pokud je v operačním systému počítače povolen režim kompatibility s federálním standardem pro zpracování informací, v operačním systému Windows 8 a ve starších verzích operačního systému se zobrazí žádost o připojení paměťového zařízení, aby byl uložen soubor obnovovacího klíče. Na jedno úložné zařízení můžete uložit více souborů klíčů pro obnovení.

Po nastavení hesla nebo kódu PIN vás BitLocker požádá o restartování počítače, kterým šifrování dokončíte. Dále musí uživatel projít ověřením nástrojem BitLocker. Po ověření se musí uživatel přihlásit k systému. Po načtení operačního systému BitLocker dokončí šifrování.

Pokud není k dispozici žádný přístup k šifrovacím klíčům, uživatel může požadovat, aby správce místní sítě zadal obnovovací klíč (pokud obnovovací klíč nebyl uložen dříve na paměťové zařízení nebo byl ztracen).

Nastavení součásti BitLocker Drive Encryption

Parametr	Popis
Povolit použití ověřování BitLocker vyžadující vstup z klávesnice před spuštěním na tabletech	Tímto zaškrtávacím políčkem lze povolit nebo zakázat použití ověřování vyžadujícího zadání dat v prostředí před spuštěním, i když platforma nemá možnost vstupu před spuštěním (například s dotykovými klávesnicemi na tabletech). V prostředí před spuštěním není k dispozici dotyková obrazovka tabletů. Aby bylo možné v tabletech dokončit ověřování pomocí technologie BitLocker, uživatel musí připojit například klávesnici USB. Je-li toto políčko zaškrtnuto, použití ověřování vyžadujícího vstup před spuštěním bude povoleno. Toto nastavení doporučujeme použít pouze pro zařízení, která mají alternativní nástroje pro zadání dat v prostředí před spuštěním, jako je například USB klávesnice kromě dotykové klávesnice. Není-li toto políčko zaškrtnuto, technologii BitLocker Drive Encryption nelze používat na tabletech.
Použít hardwarové šifrování (Windows 8 a novější verze)	Pokud je políčko zaškrtnuté, aplikace použije hardwarové šifrování. Tím se zvyšuje rychlost šifrování a bude využito méně výpočetních prostředků.
Zašifrovat pouze využité místo na disku (Windows 8 a novější verze)	Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat funkci, která omezuje oblast šifrování pouze na využité sektory pevného disku. Díky tomuto omezení lze zkrátit dobu šifrování.

	Povolení nebo zakázání funkce **Zašifrovat pouze využité místo na disku (zkracuje dobu šifrování)** po spuštění šifrování nezmění toto nastavení, dokud nebudou pevné disky zašifrované. Před zahájením šifrování je třeba políčko zaškrtnout nebo zrušit jeho zaškrtnutí. Pokud je toto políčko zaškrtnuto, budou šifrovány pouze části pevného disku, na kterých jsou soubory. Aplikace Kaspersky Endpoint Security automaticky šifruje nová data při jejich přidání. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude šifrováno celý pevný disk, včetně zbytkových fragmentů dříve odstraněných a upravených souborů. Tuto funkci doporučujeme používat u nových disků, jejichž data ještě nebyla upravena nebo odstraněna. Pokud použijete šifrování u pevného disku, který se již používá, doporučujeme šifrovat celý pevný disk. Zajistíte tím ochranu všech dat, a to i odstraněných dat, která se dají případně obnovit. Toto políčko není ve výchozím nastavení zaškrtnuto.
Nastavení ověřování	**Použít heslo (Windows 8 a novější verze)** Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security vyzve uživatele k zadání hesla, když se uživatel pokusí o přístup k šifrovanému disku. Tuto možnost lze vybrat, když není čip TPM (Trusted Platform Module) použit. **Použít čip TPM (Trusted Platform Module)** Je-li tato možnost vybrána, technologie BitLocker použije čip TPM (Trusted Platform Module). *Trusted Platform Module (TPM)* je mikročip vyvinutý pro poskytování základních funkcí souvisejících se zabezpečením (například k ukládání šifrovacích klíčů). Čip TPM je obvykle instalovaný na základní desce počítače a komunikuje se všemi ostatními součástmi systému prostřednictvím hardwarového rozhraní. U počítačů se systémem Windows 7 nebo Windows Server 2008 R2 je k dispozici pouze šifrování pomocí modulu TPM. Pokud modul TPM není nainstalován, šifrování nástroje BitLocker není možné. Použití hesla v těchto počítačích není podporováno. Zařízení vybavené čipem TPM (Trusted Platform Module) může vytvořit šifrovací klíče, které lze dešifrovat pouze pomocí tohoto zařízení. Čip TPM (Trusted Platform Module) šifruje šifrovací klíče pomocí vlastního kořenového klíče úložiště. Kořenový klíč úložiště je uložen v čipu TPM (Trusted Platform Module). Ten poskytuje další úroveň ochrany před pokusy o hacknutí šifrovacích klíčů. Tato akce je nastavena jako výchozí. Pro přístup k šifrovacímu klíči můžete nastavit další vrstvu ochranu a klíč zašifrovat heslem nebo kódem PIN: • **Použít kód PIN z TPM**. Je-li toto políčko zaškrtnuto, uživatel může použít kód PIN k získání přístupu k šifrovacímu klíči, který je uložen v čipu TPM (Trusted Platform Module). Pokud není toto zaškrtávací políčko zaškrtnuto, uživatelé nebudou moci používat kódy PIN. Pro přístup k šifrovacímu klíči musí uživatel zadat heslo. Uživateli můžete povolit používání rozšířeného kódu PIN. *Rozšířený PIN* umožňuje kromě numerických znaků používat i další znaky: velká a malá písmena latinky, speciální znaky a mezery.

	• **Použít TPM (Trusted Platform Module); pokud není k dispozici, použít heslo**. Pokud není toto políčko zaškrtnuto, uživatel může získat přístup k šifrovacím klíčům pomocí hesla, když není čip TPM (Trusted Platform Module) k dispozici. Pokud políčko není zaškrtnuto a TPM není k dispozici, úplné šifrování disku se nespustí.

Dešifrování pevného disku chráněného nástrojem BitLocker

Uživatelé mohou disk dešifrovat pomocí operačního systému (funkce *Vypnout nástroj BitLocker*). Poté aplikace Kaspersky Endpoint Security vyzve uživatele, aby disk znovu zašifroval. Aplikace Kaspersky Endpoint Security bude vyzývat k zašifrování disku, ledaže v zásadě povolíte dešifrování disku.

Jak dešifrovat pevný disk chráněný nástrojem BitLocker pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Úplné šifrování disku**.
6. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **BitLocker Drive Encryption**.
7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Dešifrovat všechny pevné disky**.
8. Uložte změny.

Jak dešifrovat pevný disk šifrovaný pomocí nástroje BitLocker prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzole vyberte kartu **Zařízení** → **Zásady a profily**.
2. U počítačů, u nichž chcete dešifrovat pevné disky, klikněte na název zásady aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Šifrování dat** → **Úplné šifrování disku**.
5. Vyberte technologii **BitLocker Drive Encryption** a po kliknutí na odkaz nakonfigurujte nastavení.

   Otevře se nastavení šifrování.
6. V rozevíracím seznamu **Režim šifrování** vyberte položku **Dešifrovat všechny pevné disky**.
7. Klikněte na tlačítko **OK**.

Nástroj Sledování šifrování můžete použít k řízení procesu šifrování nebo dešifrování disku v počítači uživatele. Nástroj Sledování šifrování můžete spustit z hlavního okna aplikace.

Obnovení přístupu k pevnému disku chráněnému nástrojem BitLocker

Pokud uživatel zapomněl heslo pro přístup k pevnému disku šifrovanému nástrojem BitLocker, musí zahájit proces obnovení (žádost–odpověď).

Pokud je v operačním systému počítače povolen režim kompatibility s federálním standardem pro zpracování informací, pak se v systému Windows 8 a starších soubor klíčů pro obnovení uloží na vyměnitelnou jednotku před šifrováním. Chcete-li obnovit přístup k jednotce, vložte vyměnitelnou jednotku a postupujte podle pokynů na obrazovce.

Obnovení přístupu k pevnému disku zašifrovanému pomocí nástroje BitLocker se skládá z následujících kroků:

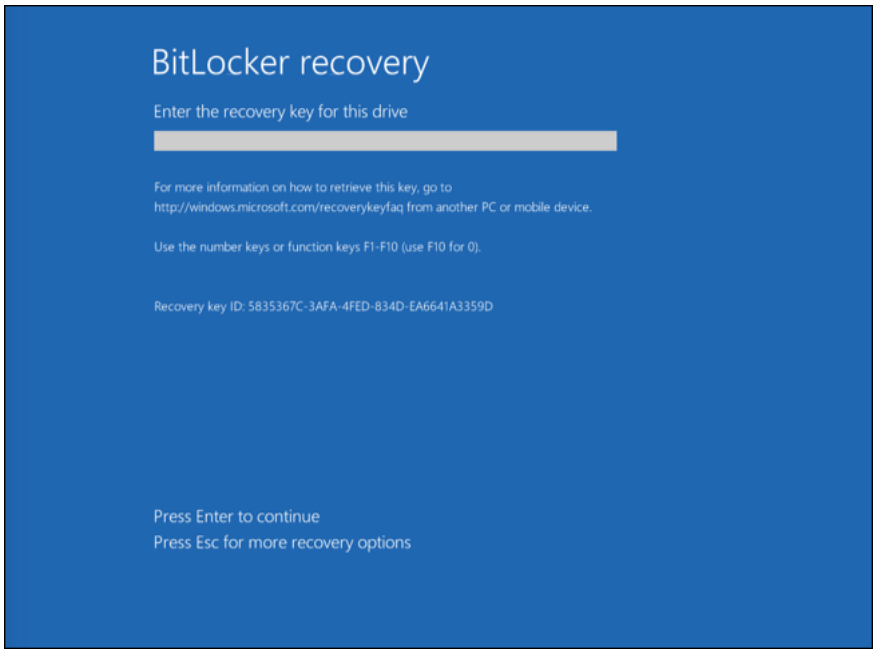
1. Uživatel sdělí správci ID obnovovacího klíče (viz obrázek níže).
2. Správce toto ID ověří ve vlastnostech počítače v aplikaci Kaspersky Security Center. ID poskytnuté uživatelem se musí shodovat s ID zobrazeným ve vlastnostech počítače.
3. Pokud se ID obnovovacího klíče shodují, správce poskytne uživateli obnovovací klíč nebo odešle soubor obnovovacího klíče.

   Soubor obnovovacího klíče se používá pro počítače, které používají následující operační systémy:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

U všech ostatních operačních systémů se používá obnovovací klíč.

4. Uživatel zadá obnovovací klíč a získá přístup na pevný disk.



Obnovení přístupu k oevnému disku zašifrovanému nástrojem BitLocker

Obnovení přístupu k systémové jednotce

Chce-li uživatel zahájit proces obnovení, musí stisknout klávesu **Esc** ve fázi před spuštěním ověření.

[Jak zobrazit obnovovací klíč pro systémovou jednotku zašifrovanou nástrojem BitLocker v konzole pro právu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
5. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
6. V okně, které se otevře, vyberte kartu **Přístup k systémové jednotce chráněné pomocí nástroje BitLocker**.
7. Požádejte uživatele o ID obnovovacího klíče uvedené v okně pro zadání hesla BitLocker a srovnejte ho s ID v poli **ID obnovovacího klíče**.

   Pokud se ID neshodují, tento klíč není platný pro obnovení přístupu k dané systémové jednotce. Ujistěte se, že se název vybraného počítače shoduje s názvem počítače uživatele.

Díky tomu budete mít přístup k obnovovacímu klíči nebo souboru obnovovacího klíče, který bude muset být předán uživateli.

[Jak zobrazit obnovovací klíč systémové jednotky zašifrované pomocí nástroje BitLocker ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.
4. V otevřeném okně vyberte kartu **BitLocker**.
5. Ověřte ID obnovovacího klíče. ID poskytnuté uživatelem se musí shodovat s ID zobrazeným v nastavení počítače.

   Pokud se ID neshodují, tento klíč není platný pro obnovení přístupu k dané systémové jednotce. Ujistěte se, že se název vybraného počítače shoduje s názvem počítače uživatele.
6. Klikněte na tlačítko **Přijmout klíč**.

Díky tomu budete mít přístup k obnovovacímu klíči nebo souboru obnovovacího klíče, který bude muset být předán uživateli.

Po načtení operačního systému aplikace Kaspersky Endpoint Security vyzve uživatele ke změně hesla nebo kódu PIN. Po nastavení nového hesla nebo kódu PIN vytvoří nástroj BitLocker nový hlavní klíč a odešle jej do aplikace Kaspersky Security Center. Tím dojde k aktualizaci obnovovacího klíče a souboru obnovovacího klíče. Pokud uživatel heslo nezměnil, můžete při příštím načtení operačního systému použít starý klíč pro obnovení.

Počítače se systémem Windows 7 neumožňují změnu hesla ani kódu PIN. Po zadání klíče obnovení a načtení operačního systému aplikace Kaspersky Endpoint Security nebude vyzývat uživatele ke změně hesla nebo kódu PIN. Není tedy možné nastavit nové heslo ani kód PIN. Tento problém vychází ze zvláštností tohoto operačního systému. Chcete-li pokračovat, musíte znovu zašifrovat pevný disk.

Obnovení přístupu k nesystémové jednotce

Chce-li uživatel zahájit proces obnovení, musí v okně udělujícím přístup k jednotce kliknout na odkaz **Zapomenuté heslo**. Po získání přístupu k šifrované jednotce může uživatel povolit automatické odblokování jednotky během ověřování Windows v nastavení nástroje BitLocker.

Jak zobrazit obnovovací klíč pro nesystémovou jednotku zašifrovanou nástrojem BitLocker v konzole pro právu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole pro správu vyberte možnosti **Additional** → **Data encryption and protection** → složku **Encrypted devices**.
3. Vyberte v pracovním prostoru šifrované zařízení, pro které chcete vytvořit soubor přístupového klíče, a v místní nabídce zařízení vyberte možnost **Získání přístupu k zařízení v aplikaci Kaspersky Endpoint Security pro systém Windows (11.6.0)**.
4. Požádejte uživatele o ID obnovovacího klíče uvedené v okně pro zadání hesla BitLocker a srovnejte ho s ID v poli **ID obnovovacího klíče**.

   Pokud se ID neshodují, tento klíč není platný pro obnovení přístupu k dané jednotce. Ujistěte se, že se název vybraného počítače shoduje s názvem počítače uživatele.

5. Odešlete uživateli klíč uvedený v poli **Obnovovací klíč**.

Jak zobrazit obnovovací klíč nesystémové jednotky zašifrované pomocí nástroje BitLocker ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Operace → Šifrování dat a ochrana → Šifrovaná zařízení**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.

   Tím se spustí průvodce pro udělení přístupu k zařízení.
4. Při udělování přístupu k zařízení postupujte podle pokynů průvodce:
   a. Vyberte modul plug-in aplikace **Kaspersky Endpoint Security pro systém Windows**.
   b. Ověřte ID obnovovacího klíče. ID poskytnuté uživatelem se musí shodovat s ID zobrazeným v nastavení počítače.

      Pokud se ID neshodují, tento klíč není platný pro obnovení přístupu k dané systémové jednotce. Ujistěte se, že se název vybraného počítače shoduje s názvem počítače uživatele.
   c. Klikněte na tlačítko **Přijmout klíč**.

Díky tomu budete mít přístup k obnovovacímu klíči nebo souboru obnovovacího klíče, který bude muset být předán uživateli.

Šifrování na úrovni souborů na místních discích počítače

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Šifrování souborů má následující zvláštní funkce:

- Aplikace Kaspersky Endpoint Security šifruje/dešifruje soubory v předdefinovaných složkách jen pro místní uživatelské profily v operačním systému. Aplikace Kaspersky Endpoint Security nešifruje ani nedešifruje soubory v předdefinovaných složkách uživatelských profilů roamingu, povinných uživatelských profilů, dočasných uživatelských profilů ani soubory v přesměrovaných složkách.
- Aplikace Kaspersky Endpoint Security nešifruje soubory, jejichž změnou by mohlo dojít k poškození operačního systému a nainstalovaných aplikací. Na seznamu položek vyloučených ze šifrování jsou například následující soubory a složky se všemi vnořenými složkami:
  - %WINDIR%;
  - %PROGRAMFILES% a %PROGRAMFILES(X86)%;
  - Soubory registru systému Windows.

Seznam položek vyloučených ze šifrování nelze zobrazit ani upravit. I když lze soubory a složky, které jsou na seznamu položek vyloučených ze šifrování, přidat na seznam šifrovaných položek, během šifrování souborů se nezašifrují.

Šifrování souborů na místních počítačových discích

Aplikace Kaspersky Endpoint Security nešifruje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive, a blokuje kopírování šifrovaných souborů do cloudového úložiště OneDrive, pokud nejsou tyto soubory přidány do pravidla dešifrování.

Postup šifrování souborů na místních discích:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Šifrování na úrovni souborů**.
6. V pravé části okna vyberte kartu **Šifrování**.
7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Podle pravidel**.
8. Na kartě **Šifrování** klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte jednu z následujících položek:

   a. Vyberte položku **Předdefinované složky**, chcete-li do pravidla šifrování přidat soubory ze složek místních uživatelských profilů navržených odborníky společnosti Kaspersky.

   - **Dokumenty**. Soubory ve standardní systémové složce *Dokumenty* a jejích podsložkách.
   - **Oblíbené položky**. Soubory ve standardní systémové složce *Oblíbené položky* a jejích podsložkách.
   - **Plocha**. Soubory ve standardní systémové složce *Plocha* a jejích podsložkách.
   - **Dočasné soubory**. Dočasné soubory související s provozováním aplikací nainstalovaných v počítači. Například aplikace sady Microsoft Office vytvářejí dočasné soubory obsahující záložní kopie dokumentů.
   - **Soubory aplikace Outlook**. Soubory související s provozem poštovního klienta aplikace Outlook: datové soubory (PST), offline datové soubory (OST), offline soubory adresáře (OAB) a soubory osobních adresářů (PAB).

   b. Vyberte položku **Vlastní složka**, chcete-li do pravidla šifrování přidat ručně zadanou cestu ke složce.

   Při přidávání cesty ke složce dodržujte následující pravidla:

   - Použijte proměnnou prostředí (například `%FOLDER%\UserFolder\`). Proměnnou prostředí můžete použít pouze jednou a pouze na začátku cesty.

- Nepoužívejte relativní cesty. Můžete použít sadu `\..\` (např. `C:\Users\..\UserFolder\`). Sada `\..\` označuje přechod do nadřazené složky.
- Nepoužívejte znaky `*` ani `?`.
- Nepoužívejte cesty UNC.
- Jako oddělovač znaků použijte `;` nebo `,`.

c. Chcete-li do pravidla šifrování přidat jednotlivé přípony souborů, vyberte položku **Soubory podle přípony**. Aplikace Kaspersky Endpoint Security zašifruje soubory se zadanými příponami na všech místních discích počítače.

d. Chcete-li do pravidla šifrování přidat skupiny přípon souborů (například *dokumenty aplikace Microsoft Office*), vyberte položku **Soubory podle skupin přípon**. Aplikace Kaspersky Endpoint Security zašifruje soubory s příponami uvedenými ve skupinách přípon na všech místních discích počítače.

9. Uložte změny.

Jakmile se zásady použijí, aplikace Kaspersky Endpoint Security zašifruje soubory, které jsou zahrnuté do pravidla šifrování a nejsou zahrnuté do pravidla dešifrování.

Šifrování souborů má následující zvláštní funkce:

- Pokud je stejný soubor přidán do pravidla šifrování i pravidla dešifrování, provede aplikace Kaspersky Endpoint Security následující akce:
  - Pokud soubor není zašifrovaný, aplikace Kaspersky Endpoint Security tento soubor nešifruje.
  - Je-li soubor zašifrovaný, aplikace Kaspersky Endpoint Security tento soubor dešifruje.
- Aplikace Kaspersky Endpoint Security pokračuje v šifrování nových souborů, pokud tyto soubory splňují kritéria pravidla šifrování. Například když změníte vlastnosti nešifrovaného souboru (cesta nebo přípona), pak soubor splňuje kritéria pravidla šifrování. Aplikace Kaspersky Endpoint Security tento soubor zašifruje.
- Když uživatel vytvoří nový soubor s vlastnostmi, které splňují kritéria pravidla šifrování, aplikace Kaspersky Endpoint Security tento soubor zašifruje, jakmile bude otevřen.
- Aplikace Kaspersky Endpoint Security odloží šifrování otevřených souborů na dobu, kdy budou soubory zavřeny.
- Pokud přesunete šifrovaný soubor do jiné složky na místním disku, tento soubor zůstane zašifrovaný bez ohledu na to, zda je či není daná složka do pravidla šifrování zahrnutá.
- Pokud dešifrujete soubor a zkopírujete jej do jiné místní složky, která není součástí pravidla dešifrování, může být kopie souboru šifrována. Chcete-li zabránit šifrování kopírovaného souboru, vytvořte dešifrovací pravidlo pro cílovou složku.

Vytvoření pravidel přístupu k šifrovaným souborům pro aplikace

Postup vytvoření pravidel přístupu k šifrovaným souborům pro aplikace:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.

3. V pracovním prostoru vyberte kartu **Policies**.

4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

5. V okně zásad vyberte možnost **Šifrování dat → Šifrování na úrovni souborů**.

6. V rozevíracím seznamu **Režim šifrování** vyberte položku **Podle pravidel**.

   Pravidla přístupu se použijí jen při zapnutém režimu **Podle pravidel**. Pokud po použití pravidel přístupu v režimu **Podle pravidel** přepnete na režim **Ponechat bez změny**, aplikace Kaspersky Endpoint Security bude ignorovat všechna pravidla přístupu. Všechny aplikace budou mít přístup ke všem šifrovaným souborům.

7. V pravé části okna vyberte kartu **Pravidla pro aplikace**.

8. Pokud chcete vybrat aplikace jen ze seznamu aplikace Kaspersky Security Center, klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte položku **Aplikace ze seznamu aplikace Kaspersky Security Center**.

   a. Zadáním filtrů upřesněte seznam aplikací v tabulce. Lze to provést zadáním hodnot parametrů **Aplikace**, **Dodavatel** a **Období přidání** a použitím všech zaškrtávacích políček v části **Skupina**.

   b. Klikněte na tlačítko **Aktualizovat**.

   c. V tabulce se vypíšou aplikace odpovídající použitým filtrům.

   d. Ve sloupci **Aplikace** zaškrtněte políčka u aplikací, pro které chcete vytvořit pravidla přístupu k šifrovaným souborům.

   e. V rozevíracím seznamu **Pravidlo pro aplikace** vyberte pravidlo, které určí přístup aplikací k šifrovaným souborům.

   f. V rozevíracím seznamu **Dříve vybrané akce pro aplikace** vyberte akci, kterou má provést aplikace Kaspersky Endpoint Security u pravidel přístupu k šifrovaným souborům, která byla dříve pro tyto aplikace vytvořena.

   g. Klikněte na tlačítko **OK**.

   Podrobnosti o určitém pravidlu přístupu k šifrovaným souborům pro aplikaci se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

9. Pokud chcete vybrat aplikace ručně, klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte položku **Vlastní aplikace**.

   a. Zadejte do vstupního pole název nebo seznam názvů spustitelných souborů aplikací společně s jejich příponami.

      Názvy spustitelných souborů aplikací můžete také přidat ze seznamu aplikace Kaspersky Security Center tak, že kliknete na tlačítko **Přidat ze seznamu aplikace Kaspersky Security Center**.

   b. Je-li to třeba, v poli **Popis** zadejte popis seznamu aplikací.

   c. V rozevíracím seznamu **Pravidlo pro aplikace** vyberte pravidlo, které určí přístup aplikací k šifrovaným souborům.

d. Klikněte na tlačítko **OK**.

Podrobnosti o určitém pravidlu přístupu k šifrovaným souborům pro aplikaci se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

10. Uložte změny.

Šifrování souborů vytvořených nebo upravených konkrétními aplikacemi

Můžete vytvořit pravidlo, podle kterého bude aplikace Kaspersky Endpoint Security šifrovat všechny soubory vytvořené nebo upravené aplikacemi určenými v rámci pravidla.

Soubory vytvořené nebo upravené určenými aplikacemi před použitím pravidla šifrování nebudou zašifrovány.

Postup konfigurace šifrování souborů vytvořených nebo upravených konkrétními aplikacemi:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat → Šifrování na úrovni souborů**.
6. V rozevíracím seznamu **Režim šifrování** vyberte položku **Podle pravidel**.

   Pravidla šifrování jsou používána pouze v režimu **Podle pravidel**. Pokud po použití pravidel šifrování v režimu **Podle pravidel** přepnete na režim **Ponechat bez změny**, aplikace Kaspersky Endpoint Security bude ignorovat všechna pravidla šifrování. Soubory, které byly dříve zašifrovány, zůstanou zašifrovány.

7. V pravé části okna vyberte kartu **Pravidla pro aplikace**.
8. Pokud chcete vybrat aplikace jen ze seznamu aplikace Kaspersky Security Center, klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte položku **Aplikace ze seznamu aplikace Kaspersky Security Center**.

   Otevře se okno **Přidat aplikace ze seznamu aplikace Kaspersky Security Center**.

   Postupujte následovně:

   a. Zadáním filtrů upřesněte seznam aplikací v tabulce. Lze to provést zadáním hodnot parametrů **Aplikace**, **Dodavatel** a **Období přidání** a použitím všech zaškrtávacích políček v části **Skupina**.

   b. Klikněte na tlačítko **Aktualizovat**.

      V tabulce se vypíšou aplikace odpovídající použitým filtrům.

   c. Ve sloupci **Aplikace** zaškrtněte políčka vedle aplikací, jejichž vytvořené soubory chcete šifrovat.

   d. V rozevíracím seznamu **Pravidlo pro aplikace** vyberte položku **Šifrovat všechny vytvořené soubory**.

e. V rozevíracím seznamu **Dříve vybrané akce pro aplikace** vyberte akci, kterou má provést aplikace Kaspersky Endpoint Security u pravidel šifrování souborů, která byla dříve pro tyto aplikace vytvořena.

f. Klikněte na tlačítko **OK**.

Informace o pravidle šifrování pro soubory vytvořené nebo upravené vybranými aplikacemi se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

9. Pokud chcete vybrat aplikace ručně, klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte položku **Vlastní aplikace**.

   Otevře se okno **Přidat/upravit názvy spustitelných souborů aplikací**.

   Postupujte následovně:

   a. Zadejte do vstupního pole název nebo seznam názvů spustitelných souborů aplikací společně s jejich příponami.

      Názvy spustitelných souborů aplikací můžete také přidat ze seznamu aplikace Kaspersky Security Center tak, že kliknete na tlačítko **Přidat ze seznamu aplikace Kaspersky Security Center**.

   b. Je-li to třeba, v poli **Popis** zadejte popis seznamu aplikací.

   c. V rozevíracím seznamu **Pravidlo pro aplikace** vyberte položku **Šifrovat všechny vytvořené soubory**.

   d. Klikněte na tlačítko **OK**.

   Informace o pravidle šifrování pro soubory vytvořené nebo upravené vybranými aplikacemi se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

10. Uložte změny.

Generování pravidla dešifrování

Postup generování pravidla dešifrování:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat → Šifrování na úrovni souborů**.
6. V pravé části okna klikněte na kartu **Dešifrování**.
7. V rozevíracím seznamu **Režim šifrování** vyberte položku **Podle pravidel**.
8. Na kartě **Dešifrování** klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte jednu z následujících položek:

   a. Vyberte položku **Předdefinované složky**, chcete-li do pravidla dešifrování přidat soubory ze složek místních uživatelských profilů navržených odborníky společnosti Kaspersky.

b. Vyberte položku **Vlastní složka**, chcete-li do pravidla dešifrování přidat ručně zadanou cestu ke složce.

c. Chcete-li do pravidla dešifrování přidat jednotlivé přípony souborů, vyberte položku **Soubory podle přípony**. Aplikace Kaspersky Endpoint Security nezašifruje soubory se zadanými příponami na všech místních discích počítače.

d. Chcete-li do pravidla dešifrování přidat skupiny přípon souborů (například *dokumenty aplikace Microsoft Office*), vyberte položku **Soubory podle skupin přípon**. Aplikace Kaspersky Endpoint Security nezašifruje soubory s příponami uvedenými ve skupinách přípon na všech místních discích počítače.

9. Uložte změny.

Pokud je stejný soubor přidán do pravidla šifrování a pravidla dešifrování, aplikace Kaspersky Endpoint Security takový soubor nezašifruje (pokud je nezašifrovaný) a v případě, že je takový soubor šifrovaný, dešifruje jej.

Dešifrování souborů na místních počítačových discích

Postup dešifrování souborů na místních discích:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat → Šifrování na úrovni souborů**.
6. V pravé části okna vyberte kartu **Šifrování**.
7. Odeberte ze seznamu položek k šifrování soubory a složky, které chcete dešifrovat. To provedete tak, že vyberete soubory a potom zvolíte v kontextové nabídce tlačítka **Odebrat** položku **Odstranit pravidlo a dešifrovat soubory**.

   Ze seznamu položek k šifrování můžete odstranit více položek najednou. To provedete tak, že podržíte stisknutou klávesu **CTRL** a současně vyberete požadované soubory kliknutím levým tlačítkem myši a potom zvolíte v kontextové nabídce tlačítka **Odebrat** položku **Odstranit pravidlo a dešifrovat soubory**.

   Soubory a složky odebrané ze seznamu položek k šifrování jsou automaticky přidány na seznam položek k dešifrování.

8. Vytvořte seznam souborů k dešifrování.
9. Uložte změny.

Jakmile se zásady použijí, aplikace Kaspersky Endpoint Security dešifruje šifrované soubory přidané na seznam položek k dešifrování.

Aplikace Kaspersky Endpoint Security dešifruje šifrované soubory, pokud se jejich parametry (cesta k souboru, název souboru, přípona souboru) změní tak, že budou odpovídat parametrům objektů přidaných na seznam položek k dešifrování.

Aplikace Kaspersky Endpoint Security odloží dešifrování otevřených souborů na dobu, kdy budou soubory zavřeny.

Vytvoření šifrovaných balíčků

Chcete-li chránit svá data při odesílání souborů uživatelům mimo podnikovou síť, můžete použít šifrované balíčky. Šifrované balíčky mohou být výhodné pro přenos velkých souborů na vyměnitelných jednotkách, protože e-mailoví klienti mají omezení velikosti souborů.

Před vytvořením šifrovaných balíčků aplikace Kaspersky Endpoint Security vyzve uživatele k zadání hesla. Chcete-li spolehlivě chránit data, můžete povolit kontrolu síly hesla a zadat požadavky na sílu hesla. To zabrání uživatelům používat krátká a jednoduchá hesla, například `1234`.

Jak povolit kontrolu síly hesla při vytváření šifrovaných archivů v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Běžné nastavení šifrování**.
6. V bloku **Nastavení hesla** klikněte na tlačítko **Nastavení**.
7. V okně, které se otevře, vyberte kartu **Šifrované balíčky**.
8. Nakonfigurujte nastavení složitosti hesla při vytváření šifrovaných balíčků.

Jak povolit kontrolu síly hesla při vytváření šifrovaných archivů ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete povolit kontrolu síly hesla.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte do části **Šifrování dat** → **Šifrování na úrovni souborů**.
5. V bloku **Nastavení hesla pro šifrované balíčky** nakonfigurujte kritéria síly hesla požadovaná při vytváření šifrovaných balíčků.

Šifrované balíčky můžete vytvářet v počítačích s nainstalovanou aplikací Kaspersky Endpoint Security s dostupným šifrováním na úrovni souborů.

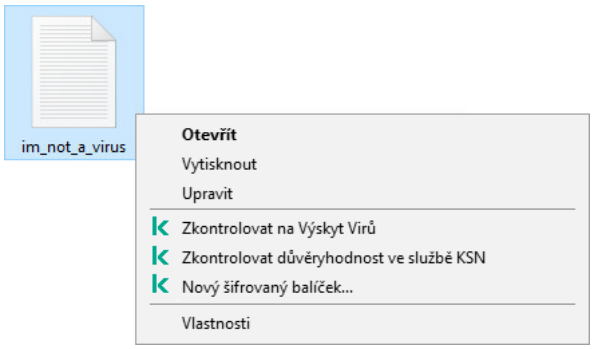
Během přidávání souboru do šifrovaného balíčku, jehož obsah je umístěn v cloudovém úložišti OneDrive, aplikace Kaspersky Endpoint Security stáhne obsah souboru a provede šifrování.

Postup vytvoření šifrovaného balíčku:

1. V libovolném správci souborů vyberte soubory nebo složky, které chcete přidat do šifrovaného balíčku. Kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
2. V kontextové nabídce vyberte položku **Nový šifrovaný balíček** (viz obrázek níže).
3. V okně, které se otevře, vyberte umístění na vyměnitelné jednotce pro uložení šifrovaného balíčku → zadejte název balíčku a klikněte na tlačítko **Uložit**.
4. V okně, které se otevře, zadejte heslo a potvrďte jej.

   Heslo musí splňovat kritéria složitosti uvedená v zásadě.
5. Klikněte na tlačítko **Vytvořit**.

Proces vytváření šifrovaného balíčku se spustí. Aplikace Kaspersky Endpoint Security neprovádí při vytváření šifrovaného balíčku komprimaci souborů. Po dokončení procesu se ve vybrané cílové složce vytvoří samorozbalovací šifrovaný balíček chráněný heslem (spustitelný soubor s příponou .exe –).



Vytvoření šifrovaného balíčku

Chcete-li přistupovat k souborům v zašifrovaném balíčku, dvojitým kliknutím na balíček spusťte průvodce rozbalením a zadejte heslo. Pokud jste heslo zapomněli nebo ztratili, není možné je obnovit a získat přístup k souborům v zašifrovaném balíčku. Šifrovaný balíček můžete znovu vytvořit.

Blokování přístupu k šifrovaným souborům

Pokud jsou soubory šifrovány, aplikace Kaspersky Endpoint Security obdrží šifrovací klíč potřebný pro přímý přístup k šifrovaným souborům. Pomocí tohoto šifrovacího klíče získá uživatel pracující pomocí jakéhokoli uživatelského účtu systému Windows, který byl aktivní během šifrování souborů, k těmto šifrovaným souborům přímý přístup. Uživatelé, kteří chtějí získat přístup k šifrovaným souborům a používají účty systému Windows, které byly během šifrování souborů neaktivní, se musí připojit k aplikaci Kaspersky Security Center.

Šifrované soubory mohou být nepřístupné za následujících okolností:

- V počítači uživatele jsou uloženy šifrovací klíče, ale neexistuje žádné připojení k aplikaci Kaspersky Security Center pro jejich správu. V tomto případě musí uživatel požádat o přístup k šifrovaným souborům správce sítě LAN.

  Pokud není k dispozici žádný přístup k aplikaci Kaspersky Security Center, je nutné postupovat následujícím způsobem:

- Požádejte o přístupový klíč pro přístup k šifrovaným souborům na pevných discích počítače.
- Aby bylo možné získat přístup k šifrovaným souborům uloženým na vyměnitelných jednotkách, požádejte o samostatný přístupový klíč pro šifrované soubory na každé vyměnitelné jednotce.

- Součásti šifrování jsou odstraněny z počítače uživatele. V tomto případě může uživatel otevřít šifrované soubory na místních a vyměnitelných discích, ale obsah těchto souborů se zobrazí jako šifrovaný.

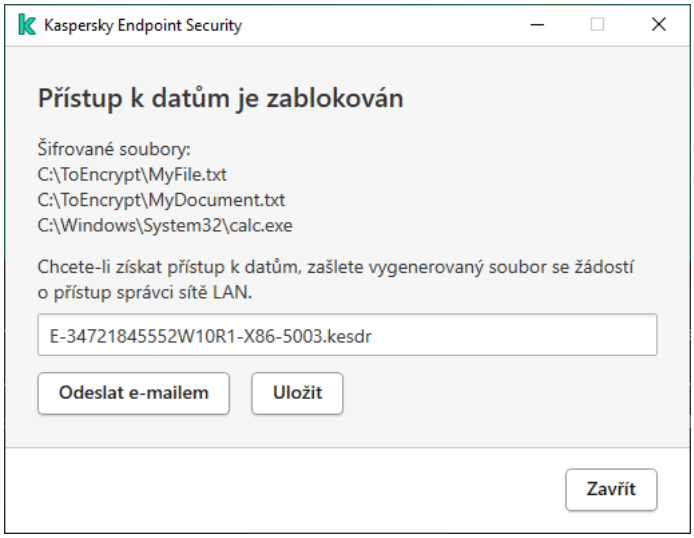
  Uživatel může se šifrovanými soubory pracovat za následujících okolností:

  - Soubory jsou umístěny uvnitř šifrovaných balíčků vytvořených v počítači s nainstalovanou aplikací Kaspersky Endpoint Security.
  - Soubory jsou uloženy na vyměnitelných jednotkách, na kterých je povolen mobilní režim.

Aby uživatel získal přístup k šifrovaným souborům, musí zahájit proces obnovení (žádost–odpověď).

Obnovení přístupu k šifrovaným souborům se skládá z následujících kroků:

1. Uživatel odešle správci soubor se žádostí o přístup (viz obrázek níže).
2. Správce přidá soubor se žádostí o přístup do aplikace Kaspersky Security Center, vytvoří soubor přístupového klíče a odešle jej uživateli.
3. Uživatel přidá soubor klíče přístupu do aplikace Kaspersky Endpoint Security a získá přístup k souborům.



Blokování přístupu k šifrovaným souborům

Chce-li uživatel zahájit proces obnovení, musí se pokusit o přístup k souboru. Aplikace Kaspersky Endpoint Security pak vytvoří soubor se žádostí o přístup (soubor s příponou KESDC), který uživatel musí zaslat správci, například e-mailem.

Aplikace Kaspersky Endpoint Security vygeneruje soubor se žádostí o přístup ke všem šifrovaným souborům uloženým na jednotce počítače (místní jednotka nebo vyměnitelná jednotka).

Jak získat soubor klíče šifrovaného přístupu k datům v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
5. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
6. V otevřeném okně vyberte kartu **Šifrování dat**.
7. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.
8. V okně pro výběr souboru se žádostí o přístup zadejte cestu k souboru přijatému od uživatele.

Zobrazí se informace o požadavku uživatele. Aplikace Kaspersky Security Center vygeneruje soubor klíče. Vygenerovaný soubor klíče šifrovaného přístupu k datům zašlete uživateli e-mailem. Případně přístupový soubor uložte a k přenosu souboru použijte libovolnou dostupnou metodu.

Jak získat soubor klíče šifrovaného přístupu k datům ve webové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.
4. Vyberte část **Šifrování dat**.
5. Klikněte na tlačítko **Vybrat soubor** a vyberte soubor se žádostí o přístup, který jste obdrželi od uživatele (soubor s příponou KESDC).

   Ve webové konzole se zobrazí informace o požadavku. Ty budou zahrnovat název počítače, na kterém uživatel požaduje přístup k souboru.
6. Klikněte na tlačítko **Uložit klíč** a vyberte složku, do které chcete uložit soubor klíče šifrovaného přístupu k datům (soubor s příponou KESDR).

Díky tomu budete moci získat soubor klíče šifrovaného přístupu k datům, který budete musíte předat uživateli.

Po přijetí souboru klíče šifrovaného přístupu k datům musí uživatel soubor spustit tak, že na něj dvakrát klikne. Aplikace Kaspersky Endpoint Security poté udělí přístup ke všem šifrovaným souborům uloženým na jednotce. Aby bylo možné získat přístup k šifrovaným souborům uloženým na jiných jednotkách, je třeba získat samostatný soubor přístupového klíče pro každou jednotku.

Obnovení přístupu k šifrovaným datům po selhání operačního systému

Po selhání operačního systému můžete obnovit přístup k datům pouze v případě šifrování na úrovni souborů (FLE). Přístup k datům nelze obnovit v případě, že je použito úplné šifrování disku (FDE).

Obnovení přístupu k šifrovaným datům po selhání operačního systému:

1. Přeinstalujte operační systém bez formátování pevného disku.
2. Nainstalujte aplikaci Kaspersky Endpoint Security.
3. Vytvořte připojení mezi počítačem a administračním serverem aplikace Kaspersky Security Center, který kontroloval počítač během šifrování dat.

Přístup k šifrovaným datům bude udělen za stejných podmínek, které platily před selháním operačního systému.

Úprava šablon zpráv pro přístup k šifrovaným souborům

Postup úpravy šablon zpráv pro přístup k šifrovaným souborům:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Běžné nastavení šifrování**.
6. V části **Šablony** klikněte na tlačítko **Šablony**.

   Otevře se okno **Šablony**.
7. Postupujte následovně:

   - Chcete-li upravit šablonu uživatelské zprávy, vyberte kartu **Zpráva uživatele**. Okno **Přístup k datům je zablokován** se otevře, když se uživatel pokusí o přístup k šifrovanému souboru a v počítači není k dispozici žádný klíč pro přístup k šifrovaným souborům. Kliknutím na tlačítko **Odeslat e-mailem** v okně **Přístup k datům je zablokován** se uživatelská zpráva automaticky vytvoří. Tato zpráva se odešle správci podnikové sítě LAN společně se souborem žádosti o přístup k šifrovaným souborům.

   - Chcete-li upravit šablonu zprávy pro správce, vyberte kartu **Administrator's message**. Tato zpráva se vytvoří automaticky při kliknutí na tlačítko **Odeslat e-mailem** v okně **Požádat o přístup k šifrovaným souborům** a je odeslána uživateli poté, co mu je udělen přístup k šifrovaným souborům.
8. Upravte šablony zpráv.

   Můžete použít tlačítko **Výchozí režim** a rozevírací seznam **Proměnná**.
9. Uložte změny.

Šifrování vyměnitelných jednotek

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Aplikace Kaspersky Endpoint Security podporuje šifrování souborů v souborových systémech FAT32 a NTFS. Pokud je k počítači připojena vyměnitelná jednotka s nepodporovaným souborovým systémem, úloha šifrování pro tuto vyměnitelnou jednotku skončí chybou a aplikace Kaspersky Endpoint Security přiřadí vyměnitelné jednotce stav jen pro čtení.

Chcete-li chránit data na vyměnitelných jednotkách, můžete použít následující typy šifrování:

- Úplné šifrování disku (FDE).

  Šifrování celé vyměnitelné jednotky, včetně systému souborů.

  Není možné přistupovat k šifrovaným datům mimo podnikovou síť. Je také nemožné přistupovat k šifrovaným datům v podnikové síti, pokud počítač není připojen k aplikaci Kaspersky Security Center (např. na hostovaném počítači).

- Šifrování na úrovni souborů (FLE).

  Šifrování pouze souborů na vyměnitelné jednotce. Systém souborů zůstává nezměněn.

  Šifrování souborů na vyměnitelných jednotkách umožňuje získat přístup k datům mimo podnikovou síť pomocí zvláštního režimu s názvem *přenosný režim*.

Během šifrování vytvoří aplikace Kaspersky Endpoint Security hlavní klíč. Aplikace Kaspersky Endpoint Security ukládá hlavní klíč do následujících úložišť:

- Kaspersky Security Center.
- Počítač uživatele.

  Hlavní klíč je šifrován tajným klíčem uživatele.

- Vyměnitelná jednotka.

  Hlavní klíč je šifrován veřejným klíčem aplikace Kaspersky Security Center.

Po dokončení šifrování jsou data na vyměnitelné jednotce přístupná v podnikové síti, jako kdyby byla na běžné nešifrované vyměnitelné jednotce.

Přístup k šifrovaným datům

Po připojení vyměnitelné jednotky se šifrovanými daty provádí aplikace Kaspersky Endpoint Security následující akce:

1. Vyhledá hlavní klíč v místním úložišti v počítači uživatele.

   Pokud je nalezen hlavní klíč, získá uživatel přístup k datům na vyměnitelné jednotce.

   Pokud hlavní klíč není nalezen, provede Kaspersky Endpoint Security následující akce:

a. Odešle žádost do aplikace Kaspersky Security Center.

   Po přijetí žádosti aplikace Kaspersky Security Center odešle odpověď, která obsahuje hlavní klíč.

b. Aplikace Kaspersky Endpoint Security uloží hlavní klíč do místního úložiště v počítači uživatele pro následné operace se šifrovanou vyměnitelnou jednotkou.

2. Dešifruje data.

Zvláštní funkce šifrování vyměnitelné jednotky

Šifrování vyměnitelných jednotek má následující speciální funkce:

- Zásady s nastavením předvoleb pro šifrování vyměnitelných jednotek se vytváří pro určitou skupinu spravovaných počítačů. Proto je výsledek použití zásady aplikace Kaspersky Security Center nakonfigurované pro šifrování/dešifrování vyměnitelných jednotek závislý na počítači, ke kterému je vyměnitelná jednotka připojená.
- Aplikace Kaspersky Endpoint Security nešifruje ani nedešifruje soubory, které jsou na vyměnitelných jednotkách ve stavu jen pro čtení.
- Následující typy zařízení jsou podporována jako vyměnitelné jednotky:
  - datová média připojená přes sběrnici USB;
  - pevné disky připojené přes sběrnice USB a FireWire;
  - jednotky SSD připojené přes sběrnice USB a FireWire.

Spuštění šifrování vyměnitelných jednotek

Pomocí zásady můžete dešifrovat vyměnitelnou jednotku. Pro konkrétní skupinu správy je generována zásada s definovaným nastavením pro šifrování vyměnitelných jednotek. Proto je výsledek dešifrování dat na vyměnitelných jednotkách závislý na počítači, ke kterému je daná vyměnitelná jednotka připojená.

Aplikace Kaspersky Endpoint Security podporuje šifrování v souborových systémech FAT32 a NTFS. Pokud je k počítači připojena vyměnitelná jednotka s nepodporovaným souborovým systémem, šifrování pro tuto vyměnitelnou jednotku skončí chybou a aplikace Kaspersky Endpoint Security přiřadí vyměnitelné přístup jen pro čtení.

Postup šifrování vyměnitelných jednotek:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat → Šifrování vyměnitelných jednotek**.

6. V části **Režim šifrování** vyberte výchozí akci, kterou má aplikace Kaspersky Endpoint Security provádět na vyměnitelných jednotkách:

   - **Šifrovat celou vyměnitelnou jednotku**. Aplikace Kaspersky Endpoint Security šifruje obsah vyměnitelné jednotky podle jednotlivých sektorů. Výsledkem je, že aplikace šifruje nejen soubory uložené na vyměnitelné jednotce, ale také jeho souborové systémy, včetně názvů souborů a struktur složek na vyměnitelné jednotce.

   - **Šifrovat všechny soubory** (FLE). Aplikace Kaspersky Endpoint Security šifruje všechny soubory uložené na vyměnitelných jednotkách. Aplikace nešifruje souborové systémy vyměnitelných jednotek, což se týká také názvů souborů a struktur složek.

   - **Šifrovat pouze nové soubory** (FLE). Aplikace Kaspersky Endpoint Security šifruje pouze soubory, které byly přidány na vyměnitelné jednotky nebo které byly uloženy na vyměnitelných jednotkách a byly upraveny po posledním použití zásad aplikace Kaspersky Security Center.

   Aplikace Kaspersky Endpoint Security znovu nešifruje vyměnitelné jednotky, které již byly zašifrovány.

7. Pokud chcete použít mobilní režim pro šifrování vyměnitelných jednotek, **zaškrtněte políčko** Mobilní režim.

   Přenosný režim je režim šifrování souborů (FLE) na vyměnitelných jednotkách, který poskytuje přístup k datům mimo podnikovou síť. Mobilní režim také umožňuje pracovat se šifrovanými daty v počítačích bez aplikace Kaspersky Endpoint Security.

8. Pokud chcete zašifrovat novou vyměnitelnou jednotku, doporučujeme zaškrtnout políčko **Zašifrovat pouze využité místo na disku**. Jestliže toto políčko není zaškrtnuté, aplikace Kaspersky Endpoint Security zašifruje všechny soubory, včetně zbytkových fragmentů odstraněných nebo upravených souborů.

9. Pokud chcete nakonfigurovat šifrování pro jednotlivé vyměnitelné jednotky, definujte pravidla šifrování.

10. Jestliže chcete použít úplné šifrování disků vyměnitelných jednotek v režimu offline, zaškrtněte políčko **Povolit šifrování vyměnitelné jednotky v režimu offline**.

    Režim šifrování offline je šifrování vyměnitelných jednotek (FDE), když není k dispozici připojení k aplikaci Kaspersky Security Center. Během šifrování ukládá aplikace Kaspersky Endpoint Security hlavní klíč pouze do počítače uživatele. Kaspersky Endpoint Security odešle hlavní klíč do aplikace Kaspersky Security Center během další synchronizace.

    Pokud je počítač, na kterém je uložen hlavní klíč, poškozený a data nejsou do aplikace Kaspersky Security Center odeslána, není možné získat přístup k vyměnitelné jednotce.

    Pokud je zaškrtnuté políčko **Povolit šifrování vyměnitelné jednotky v režimu offline** a není k dispozici žádné připojení k aplikaci Kaspersky Security Center, není šifrování vyměnitelné jednotky možné.

11. Uložte změny.

Jakmile po uplatnění zásady uživatel připojí vyměnitelnou jednotku nebo je-li vyměnitelná jednotka již připojena, aplikace Kaspersky Endpoint Security vyzve uživatele k potvrzení provedení šifrovací operace (viz obrázek níže).

Aplikace umožňuje provádět následující akce:

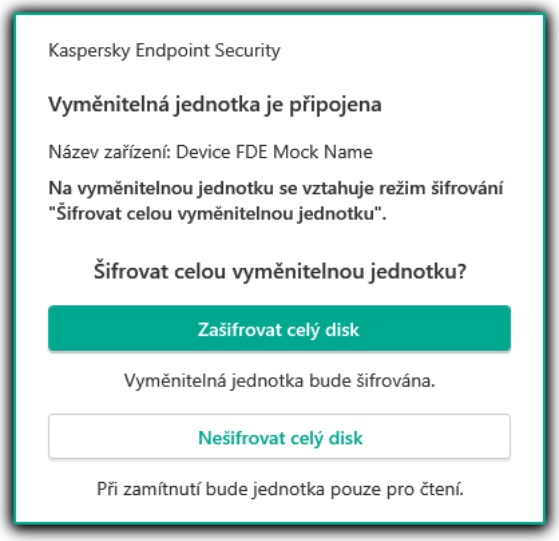
- Pokud uživatel požadavek na šifrování potvrdí, Kaspersky Endpoint Security data zašifruje.

- Pokud uživatel požadavek na šifrování odmítne, aplikace Kaspersky Endpoint Security ponechá data beze změny a přiřadí této vyměnitelné jednotce přístup pouze pro čtení.

- Jestliže uživatel na požadavek na šifrování nereaguje, aplikace Kaspersky Endpoint Security ponechá data beze změny a přiřadí této vyměnitelné jednotce přístup pouze pro čtení. Aplikace vyzve k potvrzení znovu při následném použití zásad nebo při příštím připojení této vyměnitelné jednotky.

Jestliže uživatel použije během šifrování dat funkci bezpečného odebrání vyměnitelné jednotky, aplikace Kaspersky Endpoint Security šifrování dat přeruší a umožní odebrání vyměnitelné jednotky před dokončením šifrování. Šifrování dat bude pokračovat při příštím připojení vyměnitelné jednotky k tomuto počítači.

Pokud šifrování vyměnitelné jednotky selhalo, prohlédněte si zprávu **Šifrování dat** v rozhraní Kaspersky Endpoint Security. Přístup k souborům může být zablokován jinou aplikací. V takovém případě zkuste vyměnitelnou jednotku odpojit od počítače a znovu ji připojit.



Požadavek na šifrování vyměnitelné jednotky

Přidání pravidla šifrování pro vyměnitelné jednotky

Postup přidání pravidla šifrování pro vyměnitelné jednotky:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
6. Klikněte na tlačítko **Přidat** a v rozevíracím seznamu vyberte jednu z následujících položek:
   - Pokud chcete přidat pravidla šifrování pro vyměnitelné jednotky, které jsou na seznamu důvěryhodných zařízení součásti Kontrola zařízení, vyberte položku **Ze seznamu důvěryhodných zařízení těchto zásad**.
   - Pokud chcete přidat pravidla šifrování pro vyměnitelné jednotky, které jsou na seznamu aplikace Kaspersky Security Center, vyberte položku **Ze seznamu zařízení aplikace Kaspersky Security Center**.

7. V rozevíracím seznamu **Režim šifrování pro vybraná zařízení** vyberte akci, kterou má provést aplikace Kaspersky Endpoint Security se soubory na vybraných vyměnitelných jednotkách.

8. Zaškrtněte políčko **Mobilní režim**, pokud chcete, aby aplikace Kaspersky Endpoint Security před šifrováním připravila vyměnitelné jednotky na použití šifrovaných souborů v mobilním režimu.

   Mobilní režim umožňuje používat šifrované soubory uložené na vyměnitelných jednotkách, které jsou připojené k počítačům bez funkce šifrování.

9. Zaškrtněte políčko **Zašifrovat pouze využité místo na disku**, pokud chcete, aby aplikace Kaspersky Endpoint Security šifrovala jen ty sektory disku, v nichž jsou soubory.

   Pokud chcete použít šifrování na jednotku, která se již používá, doporučujeme zašifrovat celou jednotku. Zajistíte tím ochranu veškerých dat, dokonce i odstraněných dat, která mohou obsahovat čitelné informace. Funkci **Zašifrovat pouze využité místo na disku** doporučujeme používat pro zcela nové jednotky, které nebyly předtím používány.

   Pokud bylo nějaké zařízení dříve zašifrováno pomocí funkce **Zašifrovat pouze využité místo na disku**, po použití zásad v režimu **Šifrovat celou vyměnitelnou jednotku** nebudou sektory, v nichž nejsou žádné soubory, zašifrovány.

10. V rozevíracím seznamu **Dříve vybrané akce pro zařízení** vyberte akci, kterou má provést aplikace Kaspersky Endpoint Security podle pravidel šifrování, jež byla dříve definována pro vyměnitelné jednotky:

    - Pokud chcete dříve vytvořené pravidlo šifrování pro vyměnitelnou jednotku ponechat beze změny, vyberte položku **Přeskočit**.
    - Pokud chcete dříve vytvořené pravidlo šifrování pro vyměnitelnou jednotku nahradit novým pravidlem, vyberte položku **Obnovit**.

11. Uložte změny.

Přidaná pravidla šifrování pro vyměnitelné jednotky budou použita na vyměnitelné jednotky připojené k jakýmkoli počítačům v organizaci.

Export a import seznamu pravidel šifrování pro vyměnitelné jednotky

Seznam pravidel šifrování vyměnitelné jednotky můžete exportovat do souboru XML. Poté můžete soubor upravit, například přidat velké množství pravidel pro stejný typ vyměnitelných jednotek. Funkci exportu/importu můžete také použít k zálohování seznamu pravidel nebo k migraci pravidel na jiný server.

Jak exportovat a importovat seznam pravidel šifrování vyměnitelné jednotky v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
6. Postup exportu seznamu pravidel šifrování pro vyměnitelné jednotky:
   a. Vyberte pravidla, která chcete exportovat. Chcete-li vybrat více portů, použijte klávesy **CTRL** nebo **SHIFT**.
      Pokud jste žádné pravidlo nevybrali, aplikace Kaspersky Endpoint Security exportuje všechna pravidla.
   b. Klikněte na odkaz **Exportovat**.
   c. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.
   d. Klikněte na tlačítko **Uložit**.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
7. Postup importu seznamu pravidel šifrování pro vyměnitelné jednotky:
   a. Klikněte na odkaz **Importovat**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

[Jak exportovat a importovat seznam pravidel šifrování vyměnitelné jednotky ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete exportovat nebo importovat seznam pravidel šifrování vyměnitelné jednotky.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte na část **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
5. V bloku **Pravidla šifrování pro vybraná zařízení** klikněte na odkaz **Pravidla šifrování**.

   Otevře se seznam pravidel šifrování pro vyměnitelné jednotky.
6. Postup exportu seznamu pravidel šifrování pro vyměnitelné jednotky:
   a. Vyberte pravidla, která chcete exportovat.
   b. Klikněte na tlačítko **Exportovat**.
   c. Potvrďte, jestli chcete exportovat pouze vybraná pravidla, nebo exportovat celý seznam pravidel.
   d. Klikněte na tlačítko **Exportovat**.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML ve výchozí složce pro stahování.
7. Postup importu seznamu pravidel:
   a. Klikněte na odkaz **Importovat**.

      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Klikněte na tlačítko **Otevřít**.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru TXT přidá nové položky.
8. Uložte změny.

Přenosný režim pro přístup k šifrovaným souborům na vyměnitelných jednotkách

Přenosný režim je režim šifrování souborů (FLE) na vyměnitelných jednotkách, který poskytuje přístup k datům mimo podnikovou síť. Mobilní režim také umožňuje pracovat se šifrovanými daty v počítačích bez aplikace Kaspersky Endpoint Security.

Mobilní režim je vhodný pro použití v následujících případech:

- Neexistuje žádné spojení mezi počítačem a serverem pro správu aplikace Kaspersky Security Center.
- Změnou serveru pro správu aplikace Kaspersky Security Center se změnila infrastruktura.

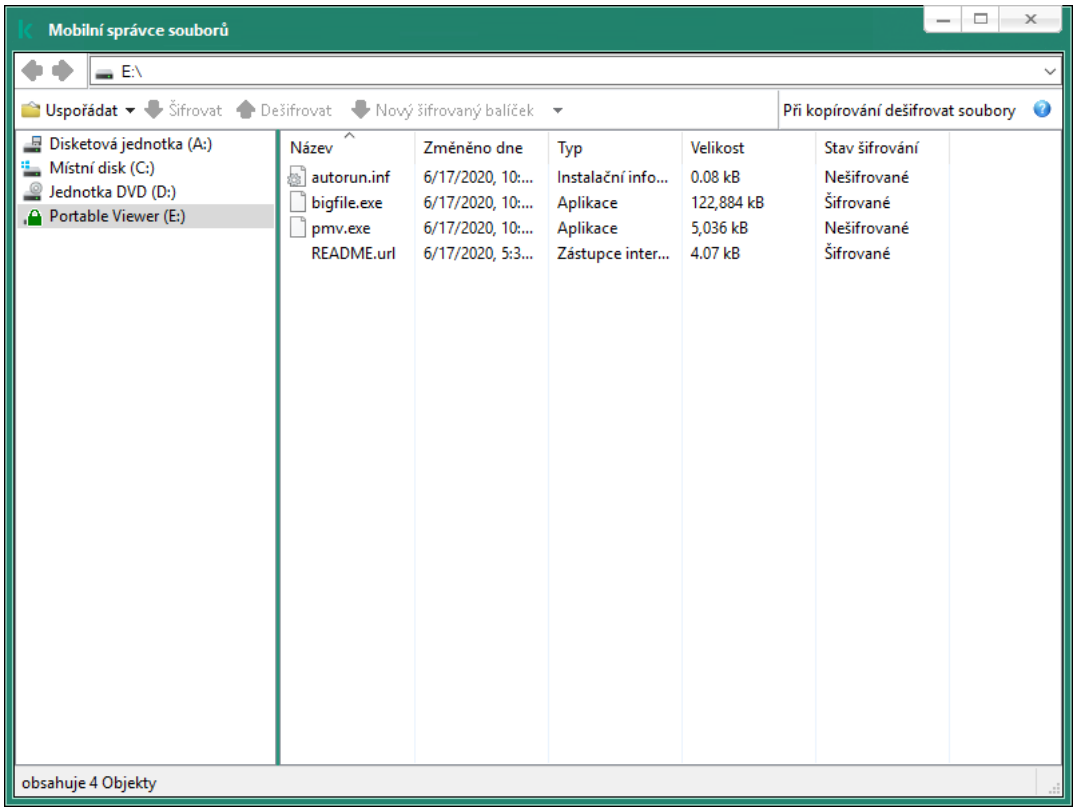
- V počítači není nainstalována aplikace Kaspersky Endpoint Security.

Mobilní správce souborů

Pro práci v mobilním režimu nainstaluje aplikace Kaspersky Endpoint Security na vyměnitelnou jednotku speciální šifrovací modul s názvem *Mobilní správce souborů*. Mobilní správce souborů poskytuje rozhraní pro práci se šifrovanými daty, pokud není v počítači nainstalována aplikace Kaspersky Endpoint Security (viz obrázek níže). Je-li ve vašem počítači nainstalována aplikace Kaspersky Endpoint Security, můžete se šifrovanými vyměnitelnými jednotkami pracovat pomocí obvyklého správce souborů (například Průzkumník).

Mobilní správce souborů ukládá klíč pro šifrování souborů na vyměnitelnou jednotku. Klíč je zašifrován pomocí hesla uživatele. Uživatel nastaví heslo před šifrováním souborů na vyměnitelné jednotce.

Správce přenosných souborů se spustí automaticky, když je vyměnitelná jednotka připojena k počítači, ve kterém není nainstalována aplikace Kaspersky Endpoint Security. Pokud je automatické spouštění aplikací v počítači zakázáno, spusťte mobilního správce souborů ručně. To provedete tak, že spustíte soubor s názvem pmv.exe, který je uložen na vyměnitelné jednotce.



Mobilní správce souborů

Podpora pro mobilní režim pro práci se šifrovanými soubory

Jak povolit podporu mobilního režimu pro práci se šifrovanými soubory na vyměnitelných jednotkách v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
6. V rozevíracím seznamu **Režim šifrování pro vybraná zařízení** vyberte možnost **Šifrovat všechny soubory** nebo **Šifrovat pouze nové soubory**.

   Mobilní režim je k dispozici pouze u šifrování na úrovni souborů (FLE). Podporu mobilního režimu nelze povolit pro úplné šifrování disku (FDE).

7. Zaškrtněte políčko **Mobilní režim**.
8. V případě potřeby přidejte pravidla šifrování pro jednotlivé vyměnitelné jednotky.
9. Uložte změny.
10. Po použití zásad připojte vyměnitelnou jednotku k počítači.
11. Potvrďte operaci šifrování vyměnitelné jednotky.

    Otevře se okno, ve kterém můžete vytvořit heslo k Mobilnímu správci souborů.

12. Zadejte heslo, které je dostatečně spolehlivé, a potvrďte jej.
13. Klikněte na tlačítko **OK**.

Aplikace Kaspersky Endpoint Security zašifruje soubory na vyměnitelné jednotce. Na vyměnitelnou jednotku bude také přidán Mobilní správce souborů používaný k práci s šifrovanými soubory. Pokud jsou na vyměnitelné jednotce již šifrované soubory, Kaspersky Endpoint Security je znovu zašifruje pomocí svého vlastního klíče. To uživateli umožňuje přístup ke všem souborům na vyměnitelné jednotce v mobilním režimu.

Jak povolit podporu mobilního režimu pro práci se šifrovanými soubory na vyměnitelných jednotkách ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Zařízení** → **Zásady a profily**.
2. Klikněte na název zásady aplikace Kaspersky Endpoint Security u počítačů, u kterých chcete povolit podporu mobilního režimu.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Nastavení aplikace**.
4. Přejděte na část **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
5. V části **Správa šifrování** vyberte možnost **Šifrovat všechny soubory** nebo **Šifrovat pouze nové soubory**.

   Mobilní režim je k dispozici pouze u šifrování na úrovni souborů (FLE). Podporu mobilního režimu nelze povolit pro úplné šifrování disku (FDE).
6. Zaškrtněte políčko **Mobilní režim**.
7. V případě potřeby přidejte pravidla šifrování pro jednotlivé vyměnitelné jednotky.
8. Uložte změny.
9. Po použití zásad připojte vyměnitelnou jednotku k počítači.
10. Potvrďte operaci šifrování vyměnitelné jednotky.

    Otevře se okno, ve kterém můžete vytvořit heslo k Mobilnímu správci souborů.
11. Zadejte heslo, které je dostatečně spolehlivé, a potvrďte jej.
12. Klikněte na tlačítko **OK**.

Aplikace Kaspersky Endpoint Security zašifruje soubory na vyměnitelné jednotce. Na vyměnitelnou jednotku bude také přidán Mobilní správce souborů používaný k práci s šifrovanými soubory. Pokud jsou na vyměnitelné jednotce již šifrované soubory, Kaspersky Endpoint Security je znovu zašifruje pomocí svého vlastního klíče. To uživateli umožňuje přístup ke všem souborům na vyměnitelné jednotce v mobilním režimu.

Přístup k šifrovaným souborům na vyměnitelné jednotce

Po zašifrování souborů na vyměnitelné jednotce s podporou mobilního režimu jsou k dispozici následující způsoby přístupu k souborům:

- Pokud není v počítači nainstalována aplikace Kaspersky Endpoint Security, Mobilní správce souborů vás vyzve k zadání hesla. Heslo budete muset zadat při každém restartování počítače nebo opětovném připojení vyměnitelné jednotky.
- Je-li počítač umístěn mimo podnikovou síť a v počítači je nainstalována aplikace Kaspersky Endpoint Security, aplikace vás vyzve k zadání hesla nebo odešle správci žádost o přístup k souborům. Po získání přístupu k souborům na vyměnitelné jednotce uloží aplikace Kaspersky Endpoint Security tajný klíč do úložiště klíčů počítače. To v budoucnu umožní přístup k souborům bez zadávání hesla nebo požádání správce.
- Nachází-li se počítač v podnikové síti a je v něm nainstalována aplikace Kaspersky Endpoint Security, získáte přístup k zařízení bez zadávání hesla. Aplikace Kaspersky Endpoint Security obdrží tajný klíč ze serveru pro

správu aplikace Kaspersky Security Center, ke kterému je počítač připojen.

Obnovení hesla pro práci v mobilním režimu

Pokud jste zapomněli heslo pro práci v mobilním režimu, musíte připojit vyměnitelnou jednotku k počítači s nainstalovanou aplikací Kaspersky Endpoint Security v podnikové síti. Přístup k souborům získáte, protože tajný klíč je uložen v úložišti klíčů počítače nebo na serveru pro správu. Dešifrujte a znovu zašifrujte soubory pomocí nového hesla.

Funkce mobilního režimu při připojování vyměnitelné jednotky k počítači z jiné sítě

Nachází-li se počítač mimo podnikovou síť a je v něm nainstalována aplikace Kaspersky Endpoint Security, získáte přístup k souborům následujícími způsoby:

- **Přístup na základě hesla**

  Po zadání hesla budete moci prohlížet, upravovat a ukládat soubory na vyměnitelnou jednotku (*transparentní přístup*). Aplikace Kaspersky Endpoint Security může pro přístup k vyměnitelné jednotce nastavit přístupové právo pouze pro čtení, pokud jsou v nastavení zásad pro šifrování vyměnitelných jednotek nakonfigurovány následující parametry:

  - Podpora přenosného režimu je zakázána.
  - Je vybrán režim **Šifrovat všechny soubory** nebo **Šifrovat pouze nové soubory**.

  Ve všech ostatních případech získáte plný přístup k vyměnitelné jednotce (oprávnění ke čtení a zápisu). Budete moci přidávat a odstraňovat soubory.

  Přístupová oprávnění k vyměnitelné jednotce můžete měnit, i když je vyměnitelná jednotka připojena k počítači. Pokud se změní přístupová oprávnění k vyměnitelné jednotce, aplikace Kaspersky Endpoint Security zablokuje přístup k souborům a znovu vás vyzve k zadání hesla.

  Po zadání hesla stavení zásad šifrování pro vyměnitelnou jednotku použít nemůžete. V tomto případě není možné soubory na vyměnitelné jednotce dešifrovat ani znovu zašifrovat.

- **Požádání správce o přístup k souborům**

  Pokud jste zapomněli heslo pro práci v mobilním režimu, požádejte správce o přístup k souborům. Pro přístup k souborům musí uživatel poslat správci soubor se žádostí o přístup (soubor s příponou KESDC). Soubor se žádostí o přístup lze poslat například e-mailem. Správce zašle soubor šifrovaného přístupu k datům (soubor s příponou KESDR).

  Po dokončení procesu žádost–odpověď pro obnovení hesla získáte transparentní přístup k souborům na vyměnitelné jednotce a plný přístup k výměnné jednotce (oprávnění ke čtení a zápisu).

  Můžete použít zásady šifrování vyměnitelné jednotky a například dešifrovat soubory. Po obnovení hesla nebo po aktualizaci zásad vás aplikace Kaspersky Endpoint Security vyzve k potvrzení změn.

  Jak získat soubor šifrovaného přístupu k datům v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.
4. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
5. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
6. V otevřeném okně vyberte kartu **Šifrování dat**.
7. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.
8. V okně pro výběr souboru se žádostí o přístup zadejte cestu k souboru přijatému od uživatele.

Zobrazí se informace o požadavku uživatele. Aplikace Kaspersky Security Center vygeneruje soubor klíče. Vygenerovaný soubor klíče šifrovaného přístupu k datům zašlete uživateli e-mailem. Případně přístupový soubor uložte a k přenosu souboru použijte libovolnou dostupnou metodu.

Jak získat soubor šifrovaného přístupu k datům ve webové konzole

1. V hlavním okně webové konzole vyberte možnosti **Devices** → **Managed devices**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.
3. Klikněte na tlačítko **Sdílet toto zařízení offline**.
4. Vyberte část **Šifrování dat**.
5. Klikněte na tlačítko **Vybrat soubor** a vyberte soubor se žádostí o přístup, který jste obdrželi od uživatele (soubor s příponou KESDC).

   Ve webové konzole se zobrazí informace o požadavku. Ty budou zahrnovat název počítače, na kterém uživatel požaduje přístup k souboru.
6. Klikněte na tlačítko **Uložit klíč** a vyberte složku, do které chcete uložit soubor klíče šifrovaného přístupu k datům (soubor s příponou KESDR).

Díky tomu budete moci získat soubor klíče šifrovaného přístupu k datům, který budete musíte předat uživateli.

Dešifrování vyměnitelných jednotek

Pomocí zásady můžete dešifrovat vyměnitelnou jednotku. Pro konkrétní skupinu správy je generována zásada s definovaným nastavením pro šifrování vyměnitelných jednotek. Proto je výsledek dešifrování dat na vyměnitelných jednotkách závislý na počítači, ke kterému je daná vyměnitelná jednotka připojená.

Postup dešifrování vyměnitelných jednotek:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Policies**.
4. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
5. V okně zásad vyberte možnost **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
6. Pokud chcete dešifrovat všechny šifrované soubory uložené na vyměnitelných jednotkách, vyberte z rozevíracího seznamu **Režim šifrování** položku **Dešifrovat celou vyměnitelnou jednotku**.
7. Chcete-li dešifrovat data uložená na jednotlivých vyměnitelných jednotkách, upravte pravidla šifrování pro vyměnitelné jednotky, jejichž data chcete dešifrovat. Postup:
   a. V seznamu vyměnitelných jednotek, pro které byla konfigurována pravidla šifrování, vyberte záznam odpovídající požadované vyměnitelné jednotce.
   b. Klikněte na tlačítko **Nastavit pravidlo** a upravte pravidlo šifrování pro vybranou vyměnitelnou jednotku.
      Otevře se kontextová nabídka tlačítka **Nastavit pravidlo**.
   c. V kontextové nabídce tlačítka **Nastavit pravidlo** vyberte položku **Dešifrování všech souborů**.
8. Uložte změny.

Pokud uživatel poté připojí vyměnitelnou jednotku nebo je-li již připojena, aplikace Kaspersky Endpoint Security vyměnitelnou jednotku dešifruje. Aplikace upozorní uživatele, že dešifrování může nějakou dobu trvat. Jestliže uživatel použije během dešifrování dat funkci bezpečného odebrání vyměnitelné jednotky, aplikace Kaspersky Endpoint Security dešifrování dat přeruší a umožní odebrání vyměnitelné jednotky před dokončením operace dešifrování. Dešifrování dat bude pokračovat při příštím připojení vyměnitelné jednotky k tomuto počítači.

Pokud selhalo dešifrování vyměnitelné jednotky, přečtěte si zprávu **Šifrování dat** v rozhraní aplikace Kaspersky Endpoint Security. Přístup k souborům může být zablokován jinou aplikací. V takovém případě zkuste vyměnitelnou jednotku odpojit od počítače a znovu ji připojit.

Zobrazení podrobností o šifrování dat

Během šifrování a dešifrování předává aplikace Kaspersky Endpoint Security informace o stavu parametrů šifrování použitých v klientských počítačích do aplikace Kaspersky Security Center.

Jsou možné následující hodnoty stavu šifrování:

- *Encryption policy not defined*. Zásady šifrování aplikace Kaspersky Security Center nebyly pro počítač definovány.
- *Applying policy*. V počítači probíhá šifrování a/nebo dešifrování dat.
- *Error*. Při šifrování a/nebo dešifrování dat v počítači došlo k chybě.

- *Reboot required*. Ke spuštění nebo ukončení šifrování nebo dešifrování dat v počítači je třeba restartovat operační systém.
- *Compliant with policy*. Šifrování dat v počítači bylo dokončeno za použití nastavení šifrování zadaných v zásadách aplikace Kaspersky Security Center, které byly v počítači použity.
- *Cancelled by user*. Uživatel odmítl potvrzení operace šifrování souboru na vyměnitelné jednotce.

Zobrazení stavu šifrování

Postup zobrazení stavu šifrování dat počítače:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, do které patří příslušné klientské počítače.
3. V pracovním prostoru vyberte kartu **Devices**.

   V pracovním prostoru na kartě **Devices** jsou zobrazeny vlastnosti počítačů ve vybrané skupině správy.
4. V pracovním prostoru na kartě **Devices** přesuňte posuvník zcela vpravo.
5. Pokud není zobrazen sloupec **Encryption status**:

   a. Kliknutím pravým tlačítkem otevřete kontextovou nabídku záhlaví tabulky.

   b. V kontextové nabídce vyberte v rozevíracím seznamu **View** možnost **Add/Remove columns**.

   Otevře se okno **Add/Remove columns**.

   c. V okně **Add/Remove columns** zaškrtněte políčko **Encryption status**.

   d. Klikněte na tlačítko **OK**.

Ve sloupci **Encryption status** je zobrazen stav šifrování dat v počítačích patřících do vybrané skupiny správy. Tento stav je vyhodnocený na základě informací o šifrování souborů na místních discích počítače a o úplném šifrování disku.

Zobrazení statistik šifrování na řídicích panelech aplikace Kaspersky Security Center

Postup zobrazení stavu šifrování na řídicích panelech aplikace Kaspersky Security Center:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole vyberte uzel **Administration Server – <Název počítače>**.
3. V pracovním prostoru vpravo od stromu Administration Console vyberte kartu **Statistics**.
4. Vytvořte novou stránku s podokny podrobností zobrazující statistiky šifrování dat. Postup:

   a. Na kartě **Statistics** klikněte na tlačítko **Customize view**.

Otevře se okno **Properties: Statistics**.

b. V okně **Properties: Statistics** klikněte na tlačítko **Add**.

Otevře se okno **Properties: New page**.

c. V části **General** okna **Properties: New page** zadejte název stránky.

d. V části **Details panes** klikněte na tlačítko **Add**.

Otevře se okno **New details pane**.

e. V okně **New details pane** ve skupině **Protection status** vyberte položku **Encryption of devices**.

f. Klikněte na tlačítko **OK**.

Otevře se okno **Properties: Encryption Control**.

g. V případě potřeby upravte nastavení podoken podrobností. K tomu použijte části **View** a **Devices** okna **Properties: Encryption of devices**.

h. Klikněte na tlačítko **OK**.

i. Opakujte kroky s pokyny d až h a vyberte položku **Šifrování vyměnitelných jednotek** v části **Protection status** okna **New details pane**.

Přidaná podokna podrobností se objeví na seznamu **Details panes** v okně **Properties: New page**.

j. V okně **Properties: New page** klikněte na tlačítko **OK**.

Název stránky s podokny podrobností vytvořenými v předchozím kroku se zobrazí na seznamu **Pages** okna **Properties: Statistics**.

k. V okně **Properties: Statistics** klikněte na tlačítko **Close**.

5. Na kartě **Statistics** otevřete stránku, která byla vytvořena během předchozích kroků s pokyny.

Zobrazí se podokna podrobností zobrazující stav šifrování počítačů a vyměnitelných jednotek.

Zobrazení chyb šifrování souborů na místních discích počítače

Postup zobrazení chyb šifrování souborů na místních discích počítače:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve složce **Managed devices** stromu konzole pro správu otevřete složku s názvem skupiny správy, která zahrnuje klientský počítač, jehož seznam chyb šifrování souborů chcete zobrazit.

3. V pracovním prostoru vyberte kartu **Devices**.

4. Na kartě **Devices** vyberte název počítače v seznamu a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.

5. V kontextové nabídce počítače vyberte položku **Vlastnosti**. V okně **Properties: <Název počítače>** vyberte část **Protection**.

6. V části **Protection** okna **Properties: <Název počítače>** otevřete kliknutím na odkaz **View list of data encryption errors** okno **Data encryption errors**.

Toto okno obsahuje podrobnosti o chybách šifrování souborů na místních discích počítače. Pokud dojde k opravení chyby, aplikace Kaspersky Security Center podrobnosti o chybě v okně **Data encryption errors** odstraní.

Zobrazení zprávy šifrování dat

Postup zobrazení zprávy šifrování dat:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. V uzlu **Administration Server** stromu konzole pro správu vyberte kartu **Reports**.
3. Klikněte na tlačítko **New report template**.

   Spustí se průvodce Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V okně **Select report template type** v části **Other** vyberte jednu z následujících položek:

   - **Managed device encryption status report** (Zpráva o stavu šifrování spravovaného zařízení).
   - **Mass storage device encryption status report** (Zpráva o stavu šifrování velkokapacitního paměťového zařízení).
   - **Encryption errors report** (Zpráva o chybách šifrování souborů).
   - **Report on blocked access to encrypted files** (Zpráva o blokovaném přístupu k šifrovaným souborům).

   Jakmile budete s průvodcem New Report Template Wizard hotovi, zobrazí se nová šablona zprávy v tabulce na kartě **Reports**.
5. Vyberte šablonu zprávy, která byla vytvořena během předchozích kroků s pokyny.
6. V kontextové nabídce šablony vyberte možnost **Show report**.

Spustí se proces generování zprávy. Zpráva se zobrazí v novém okně.

Práce s šifrovanými zařízeními v případě, že není k dispozici žádný přístup k nim

Získání přístupu k šifrovaným zařízením

Po uživateli může být požadována žádost o přístup k šifrovaným zařízením v následujících případech:

- Pevný disk byl šifrován v jiném počítači.
- Šifrovací klíč pro zařízení se nenachází v počítači (například při prvním pokusu o přístup k šifrované vyměnitelné jednotce v počítači) a počítač není připojen k aplikaci Kaspersky Security Center.

  Jakmile uživatel použije přístupový klíč na šifrované zařízení, aplikace Kaspersky Endpoint Security uloží šifrovací klíč v počítači uživatele a při dalších pokusech o přístup povolí přístup k tomuto zařízení, i když není k dispozici žádné připojení k aplikaci Kaspersky Security Center.

Přístup k šifrovaným zařízením lze získat následujícím způsobem:

1. Uživatel použije rozhraní aplikace Kaspersky Endpoint Security k vytvoření souboru se žádostí o přístup s příponou .kesdc a odešle jej správci podnikové sítě LAN.
2. Správce použije konzolu pro správu aplikace Kaspersky Security Center k vytvoření souboru přístupového klíče s příponou .kesdr a odešle jej uživateli.
3. Uživatel použije přístupový klíč.

Obnovení dat v šifrovaných zařízeních

Uživatel může použít nástroj pro obnovení šifrovaného zařízení (dále označován jako nástroj pro obnovení) k práci s šifrovanými zařízeními. Ten může být vyžadován v následujících případech:

- Postup použití přístupového klíče ke získání přístupu nebyl úspěšný.
- V počítači s šifrovaným zařízením nebyly nainstalovány součásti šifrování.

Data potřebná k obnovení přístupu k šifrovaným zařízením pomocí nástroje pro obnovení jsou po určitou dobu uložena v paměti počítače uživatele v nezašifrované podobě. Chcete-li snížit riziko neoprávněného přístupu k těmto datům, doporučuje se obnovit přístup k šifrovaným zařízením v důvěryhodných počítačích.

Data v šifrovaných zařízeních lze obnovit následujícím způsobem:

1. Uživatel použije nástroj pro obnovení k vytvoření souboru se žádostí o přístup s příponou .fdertc a odešle jej správci podnikové sítě LAN.
2. Správce použije konzolu pro správu aplikace Kaspersky Security Center k vytvoření souboru přístupového klíče s příponou .fdertr a odešle jej uživateli.
3. Uživatel použije přístupový klíč.

Aby uživatel obnovil data na šifrovaných systémových pevných discích, může také zadat přihlašovací údaje účtu ověřovacího agenta v nástroji pro obnovení. Pokud byla poškozena metadata účtu ověřovacího agenta, uživatel musí dokončit postup obnovení pomocí souboru s žádostí o přístup.

Před obnovením dat v šifrovaných zařízeních se doporučuje zrušit zásady aplikace Kaspersky Security Center nebo zakázat šifrování v nastavení zásad aplikace Kaspersky Security Center v počítači, ve kterém bude proveden postup. Tím předejdete opětovnému šifrování zařízení.

Obnova dat pomocí nástroje pro obnovení FDERT

Pokud dojde k selhání pevného disku, může být poškozen systém souborů. V takovém případě nebudou data chráněná technologií Kaspersky Disk Encryption dostupná. Data můžete dešifrovat a zkopírovat na novou jednotku.

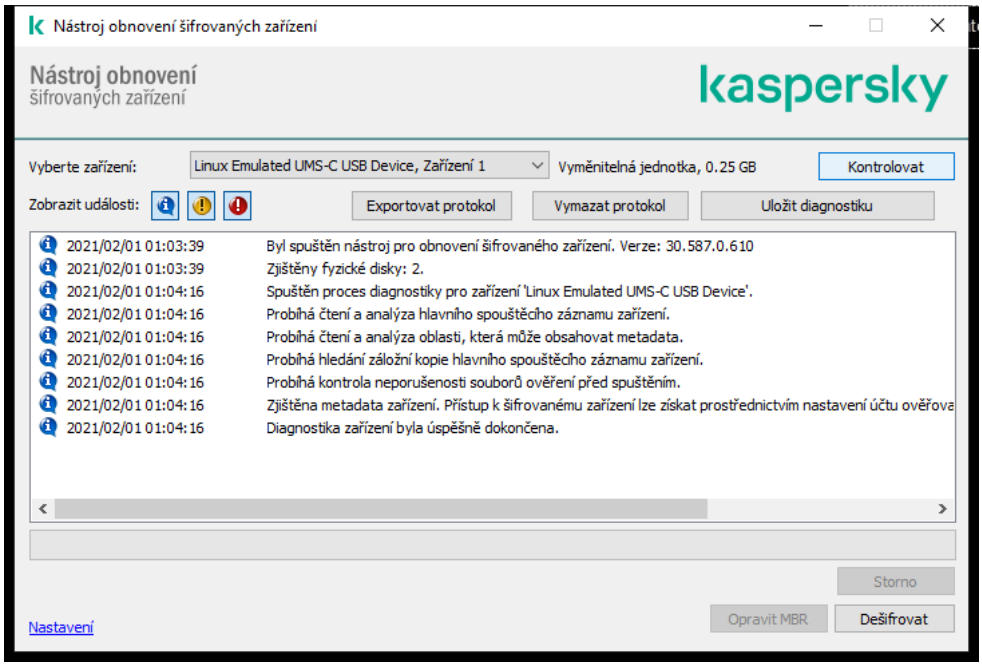
Obnovení dat a jednotce chráněné technologií Kaspersky Disk Encryption se skládá z následujících kroků:

1. Vytvořte samostatný nástroj pro obnovení (viz obrázek níže).

2. Připojte jednotku k počítači, v němž nejsou nainstalovány součásti šifrování aplikace Kaspersky Endpoint Security.

3. Spusťte nástroj pro obnovení a diagnostikujte pevný disk.

4. Přistupte k datům na jednotce. Chcete-li tak učinit, zadejte přihlašovací údaje ověřovacího agenta nebo spusťte proces obnovení (žádost–odpověď).



Nástroj pro obnovení FDERT

Vytvoření samostatného nástroje pro obnovení

Postup vytvoření spustitelného souboru nástroje pro obnovení:

1. V hlavním okně aplikace klikněte na tlačítko **Podpora**.

2. V okně, které se otevře, klikněte na tlačítko **Obnovit šifrované zařízení**.

   Spustí se nástroj obnovení šifrovaného zařízení.

3. V okně nástroje pro obnovení klikněte na tlačítko **Vytvořit samostatný nástroj pro obnovení**.

4. Uložte samostatný nástroj pro obnovení do paměti počítače.

   Spustitelný soubor nástroje obnovení (fdert.exe) se tím uloží do zadané složky. Zkopírujte nástroj pro obnovení do počítače, v němž nejsou nainstalovány součásti šifrování aplikace Kaspersky Endpoint Security. Tím předejdete opětovnému šifrování jednotky.

Data potřebná k obnovení přístupu k šifrovaným zařízením pomocí nástroje pro obnovení jsou po určitou dobu uložena v paměti počítače uživatele v nezašifrované podobě. Chcete-li snížit riziko neoprávněného přístupu k těmto datům, doporučuje se obnovit přístup k šifrovaným zařízením v důvěryhodných počítačích.

Obnovení dat na pevném disku

Postup obnovení přístupu k šifrovanému zařízení pomocí nástroje pro obnovení:

1. Spusťte soubor s názvem fdert.exe, který je spustitelným souborem nástroje pro obnovení. Tento soubor byl vytvořen aplikací Kaspersky Endpoint Security.

2. V okně nástroje pro obnovení vyberte v rozevíracím seznamu **Vyberte zařízení** šifrované zařízení, u kterého chcete obnovit přístup.

3. Kliknutím na tlačítko **Kontrola** umožníte nástroji určit akce, které se mají se zařízením provést: zda má být odemknuto nebo dešifrováno.

   Pokud má počítač přístup k funkci šifrování aplikace Kaspersky Endpoint Security, nástroj pro obnovení vás vyzve k odemknutí zařízení. Odemknutím zařízení nedojde k jeho dešifrování, k odemknutému zařízení je ale umožněn přímý přístup. Pokud počítač nemá přístup k funkci šifrování aplikace Kaspersky Endpoint Security, nástroj pro obnovení vás vyzve k dešifrování zařízení.

4. Pokud chcete importovat diagnostické informace, klikněte na tlačítko **Uložit diagnostiku**.

   Nástroj uloží archiv se soubory obsahujícími diagnostické informace.

5. Klikněte na tlačítko **Opravit MBR**, pokud se při diagnostice šifrovaného systémového pevného disku zobrazila zpráva o problémech, které se týkají hlavního spouštěcího záznamu (MBR) zařízení.

   Opravením hlavního spouštěcího záznamu zařízení se může urychlit získávání informací potřebných k odemknutí nebo dešifrování zařízení.

6. V závislosti na výsledcích diagnostiky klikněte na tlačítko **Odemknout** nebo **Dešifrovat**.

7. Pokud chcete obnovit data pomocí účtu ověřovacího agenta, vyberte možnost **Použít nastavení účtu ověřovacího agenta** a zadejte přihlašovací údaje ověřovacího agenta.

   Tento způsob je možný pouze v případě obnovení dat na systémovém pevném disku. Pokud byl systémový pevný disk poškozen a byla ztracena data účtu ověřovacího agenta, je nutné získat přístupový klíč od správce podnikové sítě LAN a obnovit data v šifrovaném zařízení.

8. Pokud chcete zahájit proces obnovení, postupujte takto:

   a. Vyberte možnost **Zadat přístupový klíč k zařízení ručně**.

   b. Klikněte na tlačítko **Přijmout přístupový klíč** a uložte soubor se žádostí o přístup do paměti počítače (soubor s příponou FDERTC).

   c. Soubor s žádostí o přístup odešlete správci podnikové sítě LAN.

   > Nezavírejte okno **Přijmout přístupový klíč k zařízení**, dokud neobdržíte přístupový klíč. Když toto okno otevřete znovu, nebudete moci použít přístupový klíč, který byl předtím vytvořen správcem.

   d. Přijměte a uložte přístupový soubor (soubor s příponou FDERTR) vytvořený a zaslaný správcem podnikové sítě LAN (viz pokyny níže).

   e. Stáhněte si přístupový soubor v okně **Přijmout přístupový klíč k zařízení**.

9. Pokud dešifrujete zařízení, musíte nakonfigurovat další nastavení dešifrování:

   - Určete oblast, kterou chcete dešifrovat:

     - Chcete-li dešifrovat celé zařízení, vyberte možnost **Dešifrovat celé zařízení**.

     - Chcete-li dešifrovat část dat v zařízení, vyberte možnost **Dešifrovat jednotlivé oblasti zařízení** a určete hranice oblasti dešifrování.

- Vyberte umístění zápisu dešifrovaných dat:
  - Chcete-li, aby data v původním zařízení byla přepsána dešifrovanými daty, zrušte zaškrtnutí políčka **Dešifrovat do souboru bitové kopie disku**.
  - Chcete-li, aby byla dešifrovaná data uložena odděleně od původních šifrovaných dat, zaškrtněte políčko **Dešifrovat do souboru bitové kopie disku** a pomocí tlačítka **Procházet** zadejte cestu, kam chcete soubor VHD uložit.

10. Klikněte na tlačítko **OK**.

Spustí se odemknutí nebo dešifrování zařízení.

[Jak vytvořit soubor šifrovaného přístupu k datům v konzole pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole pro správu vyberte možnosti **Additional** → **Data encryption and protection** → složku **Encrypted devices**.
3. Vyberte v pracovním prostoru šifrované zařízení, pro které chcete vytvořit soubor přístupového klíče, a v místní nabídce zařízení vyberte možnost **Získání přístupu k zařízení v aplikaci Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

   Pokud si nejste jisti, pro který počítač byl soubor se žádostí o přístup vytvořen, ve stromu konzoly pro správu vyberte možnost **Další** → složku **Šifrování a ochrana dat** a v pracovním prostoru klikněte na odkaz **Získat šifrovací klíč k zařízení v aplikaci Kaspersky Endpoint Security pro systém Windows (11.6.0)**.

4. V okně, které se otevře, vyberte šifrovací algoritmus, který chcete použít: **AES256** nebo **AES56**.

   Algoritmus šifrování dat závisí na šifrovací knihovně AES, která je součástí distribučního balíčku: *silné šifrování (AES256)* nebo *lehké šifrování (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.

5. Klikněte na tlačítko **Procházet**. V okně, které se otevře, zadejte cestu k souboru se žádostí o přístup (s příponou FDERTC) přijatému od uživatele.
6. Klikněte na tlačítko **Otevřít**.

Zobrazí se informace o požadavku uživatele. Aplikace Kaspersky Security Center vygeneruje soubor klíče. Vygenerovaný soubor klíče šifrovaného přístupu k datům zašlete uživateli e-mailem. Případně přístupový soubor uložte a k přenosu souboru použijte libovolnou dostupnou metodu.

[Jak vytvořit soubor šifrovaného přístupu k datům ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Operace** → Šifrování dat a ochrana → **Šifrovaná zařízení**.

2. Zaškrtněte políčko vedle názvu počítače, na němž chcete obnovit data.

3. Klikněte na tlačítko **Sdílet toto zařízení offline**.

   Tím se spustí průvodce pro udělení přístupu k zařízení.

4. Při udělování přístupu k zařízení postupujte podle pokynů průvodce:

   a. Vyberte modul plug-in aplikace **Kaspersky Endpoint Security pro systém Windows**.

   b. Vyberte šifrovací algoritmus, který chcete použít: **AES256** nebo **AES56**.

      Algoritmus šifrování dat závisí na šifrovací knihovně AES, která je součástí distribučního balíčku: *silné šifrování (AES256)* nebo *lehké šifrování (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.

   c. Klikněte na tlačítko **Vybrat soubor** a vyberte soubor se žádostí o přístup, který jste obdrželi od uživatele (soubor s příponou FDERTC).

   d. Klikněte na tlačítko **Uložit klíč** a vyberte složku, do které chcete uložit soubor klíče pro přístup k datům (soubor s příponou FDERTR).

Díky tomu budete moci získat soubor klíče šifrovaného přístupu k datům, který budete musíte předat uživateli.

Vytvoření záchranného disku operačního systému

Záchranný disk operačního systému může být užitečný, pokud z určitého důvodu není možný přístup k šifrovanému pevnému disku a operační systém nelze načíst.

Za použití záchranného disku můžete načíst obraz bitové kopie operačního systému Windows a obnovit přístup k šifrovanému pevnému disku pomocí nástroje pro obnovení, který je v bitové kopii operačního systému zahrnut.

Postup vytvoření záchranného disku operačního systému:

1. Vytvořte spustitelný soubor nástroje pro obnovení šifrovaného zařízení.

2. Vytvořte vlastní bitovou kopii prostředí před spuštěním systému Windows. Během vytváření bitové kopie prostředí před spuštěním systému Windows přidejte do kopie spustitelný soubor nástroje obnovení.

3. Uložte vlastní bitovou kopii prostředí před instalací systému Windows na spustitelné médium, například na disk CD nebo vyměnitelnou jednotku.

   Pokyny ohledně vytváření vlastní bitové kopie prostředí před spuštěním systému Windows najdete v nápovědě společnosti Microsoft (například v rámci sítě Microsoft TechNet).

Správa aplikace z příkazového řádku

Aplikaci Kaspersky Endpoint Security můžete spravovat z příkazového řádku. Seznam příkazů pro správu aplikace můžete zobrazit spuštěním příkazu `HELP`. Chcete-li si přečíst syntaxi konkrétního příkazu, zadejte `HELP <příkaz>`.

Zvláštní znaky v příkazu je nutno escapovat. Pro escapování znaků &, |, (,), <, >, ^ použijte znak ^ (chcete-li například použít znak `&`, zadejte `^&`). Pro escapování znaku `%` zadejte `%%`.

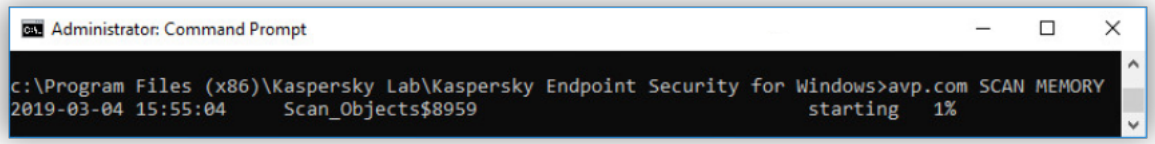
Příkazy AVP

Postup správy aplikace Kaspersky Endpoint Security z příkazového řádku:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.
3. Chcete-li provést příkaz, zadejte:

```
avp.com <příkaz> [možnosti]
```

Výsledkem je, že Kaspersky Endpoint Security provede příkaz (viz obrázek níže).



Správa aplikace z příkazového řádku

SCAN. Antivirová kontrola

Spustí úlohu antivirové kontroly.

Syntaxe příkazu

```
SCAN [<rozsah kontroly>] [<akce při zjištění hrozby>] [<typy souborů>] [<výjimky z kontroly>] [/R[A]:<soubor zprávy>] [<technologie kontroly>] [/C:< soubor s nastavením kontroly>]
```

Rozsah kontroly	
`<soubory ke kontrole>`	Seznam souborů a složek oddělených mezerami. Dlouhé cesty musí být uzavřeny v uvozovkách. Krátké cesty (formát MS-DOS) nemusí být uzavřeny v uvozovkách. Příklad:

	• `"C:\Program Files (x86)\Example Folder“` – dlouhá cesta. • `C:\PROGRA~2\EXAMPL~1` – krátká cesta.
`/ALL`	Spustí úlohu *Úplná kontrola*. Aplikace Kaspersky Endpoint Security kontroluje tyto objekty: • paměť jádra; • objekty načítané při spouštění operačního systému; • spouštěcí sektory; • zálohu operačního systému; • všechny pevné disky a vyměnitelné jednotky.
`/MEMORY`	Kontrola paměti jádra
`/STARTUP`	Kontrola objektů načítaných při spouštění operačního systému
`/MAIL`	Kontrola poštovní schránky aplikace Outlook
`/REMDRIVES`	Zkontroluje vyměnitelné jednotky.
`/FIXDRIVES`	Zkontroluje pevné disky.
`/NETDRIVES`	Zkontroluje síťové jednotky.
`/QUARANTINE`	Zkontroluje soubory v záloze aplikace Kaspersky Endpoint Security.
`/@:<seznam souborů.lst>`	Zkontroluje soubory a složky na seznamu. Každý soubor v seznamu musí být na novém řádku. Dlouhé cesty musí být uzavřeny v uvozovkách. Krátké cesty (formát MS-DOS) nemusí být uzavřeny v uvozovkách. Příklad: • `"C:\Program Files (x86)\Example Folder“` – dlouhá cesta. • `C:\PROGRA~2\EXAMPL~1` – krátká cesta.

Akce při zjištění hrozby	
`/i0`	Informovat. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb.
`/i1`	Dezinfikovat; a pokud se dezinfekce nezdaří, tak blokovat. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.
`/i2`	Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. Tato akce je nastavena jako výchozí.
`/i3`	Dezinfikujte zjištěné infikované soubory. Pokud se dezinfekce nezdaří, odstraní infikované soubory. Odstraní také složené soubory (například archivy), pokud infikovaný soubor nelze dezinfikovat nebo odstranit.

`/i4`	Odstraní infikované soubory. Odstraní také složené soubory (například archivy), pokud infikovaný soubor nelze odstranit.
`/i8`	Jakmile je zjištěna hrozba, vyzve uživatele k akci.
`/i9`	Po dokončení kontroly vyzve uživatele k akci.

Typy souborů	
`/fe`	Soubory kontrolované podle přípony. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.
`/fi`	Soubory kontrolované podle formátu. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami.
`/fa`	Všechny soubory. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje všechny soubory bez výjimky (všechny formáty a přípony). Toto je výchozí nastavení.

Výjimky z kontroly	
`-e:a`	Z rozsahu kontroly jsou vyloučeny archivy RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
`-e:b`	Z rozsahu kontroly jsou vyloučeny poštovní databáze a příchozí a odchozí e-maily.
`-E: <maska souboru>`	Z rozsahu kontroly jsou vyloučeny soubory, které odpovídají masce souboru. Příklad: • Maska `*.exe` bude reprezentovat všechny cesty k souborům, které mají příponu EXE. • Maska `example*` bude představovat všechny cesty k souborům s názvem EXAMPLE.
`-e:<sekundy>`	Z rozsahu kontroly jsou vyloučeny soubory, jejichž kontrola trvá déle, než je zadaný časový limit (v sekundách).
`-es: <megabajty>`	Z rozsahu kontroly jsou vyloučeny soubory, které jsou větší než zadaný limit velikosti (v megabajtech).

Ukládání událostí do režimu souboru zpráv	
`/R:<soubor zprávy>`	Uloží do souboru zprávy pouze kritické události.
`/RA:<soubor zprávy>`	Uloží do souboru zprávy všechny události.

Technologie kontroly	
`/iChecker=on|off`	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na

	soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).
`/iSwift=on|off`	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.

Rozšířené nastavení	
`/C:<soubor s nastavením antivirové kontroly>`	Soubor s nastavením úlohy Antivirová kontrola. Soubor musí být vytvořen ručně a uložen ve formátu TXT. Soubor může mít následující obsah: `[ <rozsah kontroly> ] [ <akce při zjištění hrozby> ] [ <typy souborů> ] [ <výjimky z kontroly> ] [/R[A]:<soubor zprávy> ] [ <technologie kontroly> ]`.

Příklad:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Aktualizace databází a softwarových modulů aplikace

Spustí úlohu *aktualizace*.

Syntaxe příkazu

```
UPDATE [local] ["<zdroj aktualizace>"] [/R[A]:<soubor zprávy>] [/C:<soubor s nastavením aktualizace>]
```

Nastavení úlohy aktualizace	
`místní`	Spuštění úlohy *Aktualizace*, která byla vytvořena automaticky po instalaci aplikace. Nastavení úlohy *Aktualizace* můžete změnit v rozhraní místní aplikace nebo v konzole aplikace Kaspersky Security Center. Pokud toto nastavení není nakonfigurováno, spustí aplikace Kaspersky Endpoint Security úlohu *Aktualizace* s výchozím nastavením nebo s nastavením uvedeným v příkazu. Nastavení úlohy aktualizace můžete nakonfigurovat následujícím způsobem: • `UPDATE` spustí úlohu *Aktualizace* s výchozím nastavením: zdroj aktualizací jsou servery aktualizace společnosti Kaspersky, účet je System a použijí se další výchozí nastavení. • `UPDATE local` spustí úlohu *Aktualizace*, která byla automaticky vytvořena po instalaci (předdefinovaná úloha). • `UPDATE <nastavení aktualizace>` spustí úlohu *Aktualizace* s ručně definovaným nastavením (viz níže).

Zdroj aktualizací	

"<zdroj aktualizací>"	Adresa serveru HTTP nebo FTP nebo sdílené složky s aktualizačním balíčkem. Můžete zadat pouze jeden zdroj aktualizace. Pokud není uveden zdroj aktualizace, použije Kaspersky Endpoint Security výchozí zdroj: aktualizační servery společnosti Kaspersky.

Ukládání událostí do režimu souboru zpráv	
/R:<soubor zprávy>	Uloží do souboru zprávy pouze kritické události.
/RA:<soubor zprávy>	Uloží do souboru zprávy všechny události.

Rozšířené nastavení	
/C:<soubor s nastavením aktualizace>	Soubor s nastavením úlohy *aktualizace*. Soubor musí být vytvořen ručně a uložen ve formátu TXT. Soubor může mít následující obsah: ["<zdroj aktualizace>"] [/R[A]:<soubor zprávy>].

Příklad:

```
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Vrácení poslední aktualizace

Vrátí zpět poslední aktualizaci antivirové databáze. To v případě potřeby umožňuje vrátit zpět moduly databází a aplikací na jejich předchozí verzi, například když nová verze databáze obsahuje neplatný podpis, který způsobí, že aplikace Kaspersky Endpoint Security zablokuje bezpečnou aplikaci.

Syntaxe příkazu

```
ROLLBACK [/R[A]:<soubor zprávy>]
```

Ukládání událostí do režimu souboru zpráv	
/R:<soubor zprávy>	Uloží do souboru zprávy pouze kritické události.
/RA:<soubor zprávy>	Uloží do souboru zprávy všechny události.

Příklad:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Trasování

Povolí/zakáže trasování. Soubory trasování jsou ukládány do počítače za předpokladu, že je aplikace používána. Po odebrání aplikace jsou soubory trvale odstraněny. Soubory trasování, kromě souborů trasování ověřovacího agenta, jsou uloženy ve složce% ProgramData%\Kaspersky Lab\KES\Traces. Ve výchozím nastavení je trasování zakázáno.

Syntaxe příkazu

```
TRACES on|off [<úroveň trasování>] [<rozšířené nastavení>]
```

Úroveň trasování	
`<úroveň trasování>`	Úroveň podrobností trasování. Dostupné hodnoty: • `100` (kritické). Pouze zprávy o závažných chybách. • `200` (vysoké). Zprávy o všech chybách, včetně závažných chyb. • `300` (diagnostické). Zprávy o všech chybách a varováních. • `400` (důležité). Všechny chybové zprávy, varování a další informace. • `500` (normální). Zprávy o všech chybách a varováních a podrobné informace o provozu aplikace v normálním režimu (výchozí). • `600` (nízké). Všechny zprávy.

Rozšířené nastavení	
`all`	Spustí příkaz pomocí parametrů `dbg`, `file` a `mem`.
`dbg`	Použije funkci OutputDebugString a uloží trasovací soubor. Funkce OutputDebugString odešle řetězec znaků do ladicího programu aplikace, který se zobrazí na obrazovce. Více informací naleznete na *webu MSDN*.
`file`	Uloží jeden soubor trasování (bez omezení velikosti).
`rot`	Uloží trasování do omezeného počtu souborů s omezenou velikostí; když je dosaženo maximální velikosti, přepíše starší soubory.
`mem`	Uloží trasování do souborů výpisu.

Příklady:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Spuštění profilu

Spustí profil (například pro aktualizaci databází nebo povolení součásti ochrany).

Syntaxe příkazu

```
START <profil> [/R[A]:<soubor zprávy>]
```

Profil	
`<profil>`	Název profilu. *Profil* je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Seznam dostupných profilů můžete zobrazit příkazem `HELP START`.

Ukládání událostí do režimu souboru zpráv	
`/R:<soubor zprávy>`	Uloží do souboru zprávy pouze kritické události.
`/RA:<soubor zprávy>`	Uloží do souboru zprávy všechny události.

Příklad:

```
avp.com START Scan_Objects
```

STOP. Zastavení profilu

Zastaví spuštěný profil (například pro zastavení kontroly, zastavení kontroly vyměnitelných jednotek nebo zakázání součásti ochrany).

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Zakázat součásti ochrany** a **Zakázat součásti kontroly**.

Syntaxe příkazu

```
STOP <profil> /login=<uživatelské jméno> /password=<heslo>
```

Profil	
`<profil>`	Název profilu. *Profil* je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Seznam dostupných profilů můžete zobrazit příkazem `HELP STOP`.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

STATUS. Stav profilu

Zobrazí informace o stavu u profilů aplikací (například `spuštěno` nebo `dokončeno`). Seznam dostupných profilů můžete zobrazit příkazem `HELP STATUS`.

Aplikace Kaspersky Endpoint Security také zobrazuje informace o stavu profilů služeb. Informace o stavu profilů služeb mohou být vyžadovány při kontaktování technické podpory společnosti Kaspersky.

Syntaxe příkazu

```
STATUS [<profil>]
```

STATISTICS. Statistiky provozu profilu

Zobrazí statistické informace o profilu aplikace (například doba trvání prověřování nebo počet zjištěných hrozeb.) Seznam dostupných profilů můžete zobrazit příkazem `HELP STATISTICS`.

Syntaxe příkazu

```
STATISTICS <profil>
```

RESTORE. Obnova souborů

Soubor můžete obnovit ze zálohy do jeho původní složky. Pokud soubor se stejným názvem již v zadané cestě existuje, k názvu souboru se připojí přípona „-kopie“. Obnovovaný soubor je zkopírován s původním názvem.

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Obnovit ze zálohy**.

Funkce *zálohování* ukládá záložní kopie souborů, které byly odstraněny nebo změněny během dezinfekce. *Záložní kopie* je kopie souboru vytvořená, předtím než byl soubor dezinfikován nebo odstraněn. Záložní kopie souborů jsou ukládány ve zvláštním formátu a nepředstavují hrozbu.

Záložní kopie souborů jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES\QB`.

Uživatelům ve skupině správců je uděleno úplné oprávnění pro přístup k této složce. Uživateli, jehož účet byl použit k instalaci aplikace Kaspersky Endpoint Security, jsou udělena omezená přístupová práva k této složce.

Aplikace Kaspersky Endpoint Security neposkytuje možnost konfigurace přístupových oprávnění uživatele za účelem zálohování kopií souborů.

Syntaxe příkazu

```
RESTORE [/REPLACE] <název souboru> / login=<uživatelské jméno> /password=<heslo>
```

Rozšířené nastavení	
`/REPLACE`	Přepíše existující soubor.
`<název souboru>`	Název souboru, který má být obnoven.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad:
`avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1`

EXPORT. Export nastavení aplikace

Export nastavení aplikace Kaspersky Endpoint Security do souboru. Soubor bude umístěn ve složce C:\Windows\SysWOW64.

Syntaxe příkazu

```
EXPORT <profil> <název souboru>
```

Profil	
`<profil>`	Název profilu. *Profil* je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Můžete zobrazit seznam dostupných profilů příkazem `HELP EXPORT`.

Soubor k exportu	
`<název souboru>`	Název souboru, do kterého se exportuje nastavení aplikace. Nastavení aplikace Kaspersky Endpoint Security můžete exportovat do konfiguračního souboru DAT nebo CFG, textového souboru TXT nebo dokumentu XML.

Příklady:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Import nastavení aplikace

Importuje nastavení aplikace Kaspersky Endpoint Security ze souboru, který byl vytvořen pomocí příkazu `EXPORT`.

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Konfigurace nastavení aplikace**.

Syntaxe příkazu

```
IMPORT <název souboru> /login=<uživatelské jméno> /password=<heslo>
```

Soubor k importu	
`<název souboru>`	Název souboru, ze kterého bude importováno nastavení aplikace. Nastavení aplikace Kaspersky Endpoint Security můžete importovat z konfiguračního souboru DAT nebo CFG, textového souboru TXT nebo z dokumentu XML.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad:
```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Použití souboru klíče

Aktivuje aplikaci Kaspersky Endpoint Security pomocí souboru klíče. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.

Syntaxe příkazu

```
ADDKEY <název souboru> /login=<uživatelské jméno> /password=<heslo>
```

Soubor klíče	
`<název souboru>`	Název souboru klíče.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu. Tyto přihlašovací údaje je třeba zadat pouze v případě, že je povolena ochrana heslem.

Příklad:
```
avp.com ADDKEY file.key
```

LICENSE. Správa licence

Provede akce s licenčními klíči aplikace Kaspersky Endpoint Security.

Chcete-li provést tento příkaz a odstranit licenční klíč, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Odstranit klíč**.

Syntaxe příkazu

```
LICENSE <operace> [/login=<uživatelské jméno> /password=<heslo>]
```

Operace	
`/ADD <název souboru>`	Aktivuje aplikaci Kaspersky Endpoint Security pomocí souboru klíče. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.
`/ADD <aktivační kód>`	Aktivuje aplikaci Kaspersky Endpoint Security pomocí aktivačního kódu. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.
`/REFRESH <název souboru>`	Obnoví licenci pomocí souboru klíče. Výsledkem této akce bude přidání rezervního klíče. Při skončení platnosti licence se stane aktivním. Spuštěním tohoto příkazu není možné přidat aktivní klíč.
`/REFRESH <aktivační kód>`	Obnoví licenci pomocí aktivačního kódu. Výsledkem této akce bude přidání rezervního klíče. Při skončení platnosti licence se stane aktivním. Spuštěním tohoto příkazu není možné přidat aktivní klíč.
`/DEL /login=<uživatelské jméno> /password=<heslo>`	Odstraní licenční klíč. Bude odstraněn i rezervní klíč.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad:

- `avp.com LICENSE /ADD file.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=KLAdmin /password=!Password1`

RENEW. Zakoupení licence

Otevře web Kaspersky, kde si můžete zakoupit nebo obnovit licenci.

PBATESTRESET. Resetování výsledků kontroly disku před šifrováním disku

Obnovení výsledků kontroly kompatibility pro Úplné šifrování disku (FDE), včetně technologií Kaspersky Disk Encryption a BitLocker Drive Encryption.

Před spuštěním úplného šifrování disku aplikace provede řadu kontrol, aby ověřila, že počítač lze šifrovat. Pokud počítač nepodporuje Úplné šifrování disku, aplikace Kaspersky Endpoint Security zaznamená informaci o nekompatibilitě. Při příštím pokusu o šifrování aplikace tuto kontrolu neprovede a upozorní vás, že šifrování není možné. Pokud se změnila hardwarová konfigurace počítače, je nutné obnovit výsledky kontroly kompatibility dříve zaznamenané aplikací, aby se znovu zkontrolovala kompatibilita pevného disku systému s technologiemi šifrování disku Kaspersky Disk Encryption a BitLocker.

EXIT. Ukončit aplikaci

Ukončí aplikaci Kaspersky Endpoint Security. Aplikace bude uvolněna z paměti RAM počítače.

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Ukončit aplikaci**.

Syntaxe příkazu

```
EXIT /login=<uživatelské jméno> /password = <heslo>
```

EXITPOLICIE. Zakázání zásad

Zakáže v počítači zásady sady softwaru Kaspersky Security Center. Všechna nastavení aplikace Kaspersky Endpoint Security jsou k dispozici pro konfiguraci, včetně nastavení, která mají v zásadách uzavřený zámek (🔒).

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Zakázat zásadu aplikace Kaspersky Security Center**.

Syntaxe příkazu

```
EXITPOLICY /login=<uživatelské jméno> /password=<heslo>
```

STARTPOLICIE. Povolení zásad

Povolí v počítači zásady sady softwaru Kaspersky Security Center. Nastavení aplikací bude nakonfigurováno podle těchto zásad.

DISABLE. Zakázání ochrany

Zakáže součást File Threat Protection v počítači, v němž vypršela licence k aplikaci Kaspersky Endpoint Security. Tento příkaz nelze spustit v počítači, který má aplikaci, která není aktivována nebo má platnou licenci.

SPYWARE. Detekce spywaru

Můžete povolit nebo zakázat detekci spywaru. Detekce spywaru je ve výchozím nastavení povolena.

Syntaxe příkazu

```
SPYWARE on|off
```

MDRLICENCE. Aktivace MDR

Proveďte operace s konfiguračním souborem BLOB a aktivujte součást Managed Detection and Response. Soubor BLOB obsahuje ID klienta a informace o licenci pro řešení Kaspersky Managed Detection and Response. Soubor BLOB je umístěn uvnitř archivu ZIP konfiguračního souboru MDR. Archiv ZIP můžete získat v konzole aplikace Kaspersky Managed Detection and Response. Podrobné informace o souboru BLOB *najdete v průvodci nápovědou k řešení Kaspersky Managed Detection and Response*.

K provádění operací se souborem BLOB jsou vyžadována oprávnění správce. Kromě toho musí být nastavení součásti Managed Detection and Response v zásadách k dispozici pro úpravy ( ).

Syntaxe příkazu

```
MDRLICENSE <operace> [/login=<uživatelské jméno> /password=<heslo>]
```

Operace	
`/ADD <název souboru>`	Konfigurační soubor BLOB se použije k integraci s aplikací Kaspersky Managed Detection and Response (formát souboru P7). Můžete použít pouze jeden soubor BLOB. Pokud byl soubor BLOB již do počítače přidán, bude nahrazen.
`/DEL`	Odstranění konfiguračního souboru BLOB.

Ověřování	
`/login=<uživatelské jméno> /password=<heslo>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad:

- `avp.com MDRLICENSE /ADD file.key`
- `avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1`

KSN. Přechod mezi globální/privátní KSN

Výběr řešení Kaspersky Security Network pro určení reputace souborů nebo webových stránek. Aplikace Kaspersky Endpoint Security podporuje následující řešení infrastruktury KSN:

- *Globální KSN* je řešení, které používá většina aplikací Kaspersky. Účastníci služby Kaspersky Security Network získávají z této služby informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází pověsti a statistik služby Kaspersky Security Network.
- *Privátní KSN* je řešení, které umožňuje uživatelům počítačů, které jsou hostiteli aplikace Kaspersky Endpoint Security nebo jiných aplikací společnosti Kaspersky, získat přístup k databázím pověsti služby Kaspersky Security Network a k dalším statistickým údajům bez odesílání dat do KSN z vlastních počítačů. Možnost privátní KSN je určena pro firemní zákazníky, kteří nemohou být součástí služby Kaspersky Security Network z některého z následujících důvodů:
  - Místní pracovní stanice nejsou připojeny k internetu.
  - Přenos jakýchkoli dat mimo zemi nebo mimo podnikovou síť LAN je zakázán zákonem nebo je omezen firemními bezpečnostními zásadami.

Syntaxe příkazu

```
KSN /global | /private <název souboru>
```

Konfigurační soubor privátní KSN		
`<název souboru>`	Název konfiguračního souboru obsahujícího nastavení proxy serveru KSN. Tento soubor má příponu PKCS7 nebo PEM.	

Příklad:

```
avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7
```

Příkazy KESCLI

Příkazy KESCLI vám umožňují získávat informace o stavu počítačové ochrany pomocí součásti OPSWAT a umožňuje vám provádět standardní úlohy, jako jsou antivirové kontroly a aktualizace databáze.

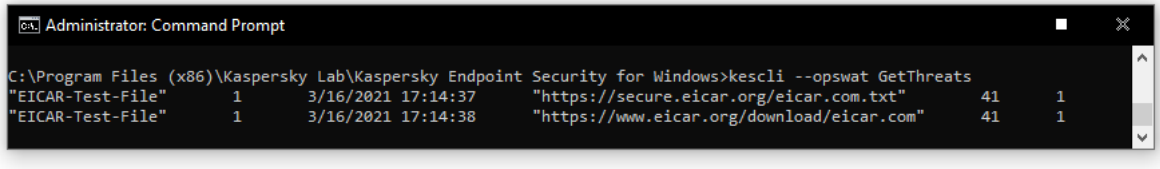
Seznam příkazů KESCLI zobrazíte příkazem `--help` nebo zkráceným příkazem `-h`.

Postup správy aplikace Kaspersky Endpoint Security z příkazového řádku:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.
3. Chcete-li provést příkaz, zadejte:

   ```
   kescli <příkaz> [možnosti]
   ```

   Výsledkem je, že Kaspersky Endpoint Security provede příkaz (viz obrázek níže).



Správa aplikace z příkazového řádku

Scan. Antivirová kontrola

Spustí úlohu antivirové kontroly.

Syntaxe příkazu

```
--opswat Scan <rozsah kontroly> <akce při zjištění hrozby>
```

Stav úlohy *Úplná kontrola* můžete zjistit příkazem `GetScanState` a datum a čas posledního dokončení kontroly příkazem `GetLastScanTime`.

Rozsah kontroly	
`<soubory ke kontrole>`	Seznam souborů a složek oddělených `;`. Např.: `C:\Program Files (x86)\příklad složky`.

Akce při zjištění hrozby	
`0`	Informovat. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb.
`1`	Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. Tato akce je nastavena jako výchozí.

Příklad:

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. Stav provádění kontroly

Získání informací o stavu provádění úlohy *Úplná kontrola*.

- `1` – kontrola probíhá.
- `0` – kontrola není spuštěna.

Syntaxe příkazu

```
--opswat GetScanState
```

Příklad:

```
kescli --opswat GetScanState
```

GetLastScanTime. Stanovení času dokončení kontroly

Získání informací o datu a času posledního dokončení úloha *Úplná kontrola*.

Syntaxe příkazu

```
--opswat GetLastScanTime
```

Příklad:

```
kescli --opswat GetLastScanTime
```

GetThreats. Získání údajů o zjištěných hrozbách

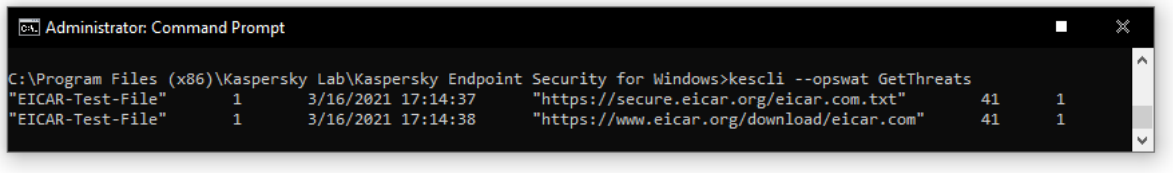
Získání seznamu zjištěných hrozeb (*zpráva o hrozbách*). Tato zpráva obsahuje informace o hrozbách a aktivitě virů za posledních 30 dní před vytvořením zprávy.

Syntaxe příkazu

```
--opswat GetThreats
```

Je-li proveden tento příkaz, aplikace Kaspersky Endpoint Security odešle odpověď v následujícím formátu:

`<název zjištěného objektu>` `<typ objektu>` `<datum a čas zjištění>` `<cesta k souboru>` `<akce při zjištění hrozby>` `<úroveň nebezpečí hrozby>`



Správa aplikace z příkazového řádku

Typ objektu	
`0`	Neznámý (`Neznámý`).
1	Virusy (`Virware`).
2	Trojské programy (`Trojware`).
3	Škodlivé programy (`Malware`).
4	Reklamní programy (`Adware`).
5	Programy automatického vytáčení (`Pornware`).
6	Aplikace, které by počítačoví zločinci mohli použít k poškození počítače nebo dat uživatele (`Riskware`).
7	Komprimované objekty, jejichž způsob komprimace může sloužit k ochraně škodlivého kódu (`Komprimované`).
20	Neznámé objekty (`Xfiles`).
21	Známé aplikace (`Software`).
22	Skryté soubory (`Skryté`).
23	Aplikace vyžadující pozornost (`Pupware`).

24	Anomální chování (`Anomálie`).
30	Nezjištěno (`Nezjištěno`).
40	Reklamní bannery (`Banner`).
50	Síťový útok (`Útok`).
51	Přístup k registru (`Registr`).
52	Podezřelá aktivita (`Podezření`).
60	Slabá místa (`Slabé místo`).
70	`Phishing`.
80	Nechtěná e-mailová příloha (`Příloha`).
90	Malware zjištěný službou Kaspersky Security Network (`Urgentní`).
100	Neznámý odkaz (`Podezřelá adresa URL`).
110	Jiný malware (`Behaviorální`).

Akce při zjištění hrozby	
0	Neznámý (`neznámý`).
1	Hrozba byla napravena (`OK`).
2	Objekt byl infikován a nebyl dezinfikován (`infikován`).
5	Objekt je v archivu a nebyl dezinfikován (`archiv`).
9	Objekt byl dezinfikován (`dezinfikován`).
10	Objekt nebyl dezinfikován (`nedezinfikován`).
11	Objekt byl odstraněn (`odstraněn`).
13	Byla vytvořena záložní kopie objektu (`zálohováno`).
15	Objekt byl přesunut do zálohy (`umístěn do karantény`).
23	Objekt byl odstraněn při restartu počítače (`odstranit při restartu`).
25	Objekt byl dezinfikován při restartu počítače (`dezinfikovat při restartu`).
29	Objekt byl přesunut do zálohy uživatelem (`přidán uživatelem`).
30	Objekt byl přidán k výjimkách (`přidán k výjimkám`).
31	Objekt byl přesunut do zálohy při restartu počítače (`umístit do karantény při restartu`).
36	Falešně pozitivní výsledek (`falešný alarm`).
38	Proces byl ukončen (`ukončen`).
40	Objekt nebyl zjištěn (`nenalezen`).
41	Hrozbu nelze vyřešit (`nelze vyřešit`).
42	Objekt byl obnoven (`vrácen zpět`).
43	Objekt byl vytvořen jako výsledek aktivity hrozby (`vytvořen hrozbou`).

`44`	Objekt byl obnoven při restartu počítače (`vrátit zpět při restartu`).
`0xffffffff`	Objekt nebyl zpracován (`zahozen`).

Úroveň rizika hrozby	
`0`	Neznámá
`1`	Vysoká
`2`	Střední kontrola
`4`	Nízká
`8`	Informační (nižší než *Nízká*)

UpdateDefinitions. Aktualizace databází a softwarových modulů aplikace

Spustí úlohu *aktualizace*. Aplikace Kaspersky Endpoint Security používá výchozí zdroj: aktualizační servery Kaspersky.

Syntaxe příkazu

```
--opswat UpdateDefinitions
```

Datum a čas naposledy dokončené úlohy *Aktualizace* můžete zobrazit příkazem `GetDefinitionsetState`.

Příklad:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Stanovení času dokončení aktualizace

Získání informací o datu a času posledního dokončení úloha *Aktualizace*.

Syntaxe příkazu

```
--opswat GetDefinitionState
```

Příklad:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Povolení ochrany

V počítači povolíte součásti ochrany aplikace Kaspersky Endpoint Security: Ochrana před souborovými hrozbami, Ochrana před webovými hrozbami, Ochrana před hrozbami v poště, Ochrana před síťovými hrozbami, Prevence narušení hostitele.

Syntaxe příkazu

```
--opswat EnableRTP
```

Provozní stav součásti Ochrana před souborovými hrozbami můžete zkontrolovat příkazem `GetRealTimeProtectionState`.

Příklad:
`kescli --opswat EnableRTP`

GetRealTimeProtectionState. Stav součásti Ochrana před souborovými hrozbami

Získání informací o provozním stavu součásti Ochrana před souborovými hrozbami:

- `1` – součást je povolena.
- `0` – součást je zakázána.

Syntaxe příkazu

```
--opswat GetRealTimeProtectionState
```

Příklad:
`kescli --opswat GetRealTimeProtectionState`

Version. Určení verze aplikace

Určení verze aplikace Kaspersky Endpoint Security pro systém Windows.

Syntaxe příkazu

```
--Version
```

Můžete rovněž použít zkrácený příkaz `-v`.

Příklad:
`kescli -v`

Chybové kódy

Při práci s aplikací prostřednictvím příkazového řádku se mohou vyskytnout chyby. Pokud dojde k chybám, aplikace Kaspersky Endpoint Security zobrazí chybovou zprávu, například `Chyba: Nelze spustit úlohu „EntAppControl“`. Aplikace Kaspersky Endpoint Security může také zobrazovat další informace ve formě kódu, například `error=8947906D` (viz tabulka níže).

Chybový kód	Popis
09479001	Licenční klíč pro aplikaci Kaspersky Endpoint Security je v tomto počítači již používán.
0947901D	Platnost licence vypršela. Aktualizace databáze není k dispozici.
89479002	Klíč nebyl nalezen.
89479003	Chybí nebo je poškozen digitální podpis.
89479004	Data jsou poškozena.
89479005	Soubor klíče je poškozen.
89479006	Platnost licence nebo platnost licenčního klíče vypršela.
89479007	Soubor klíče nebyl zadán.
89479008	Soubor klíče nelze použít.
89479009	Uložení dat se nezdařilo.
8947900A	Čtení dat se nezdařilo.
8947900B	Chyba I/O.
8947900C	Databáze nebyly nalezeny.
8947900E	Nebyla načtena knihovna licencí.
8947900F	Databáze jsou poškozeny nebo aktualizovány ručně.
89479010	Databáze jsou poškozeny.
89479011	Pro přidání rezervního klíče nelze použít neplatný soubor klíče.
89479012	Chyba systému.
89479013	Seznam zakázaných klíčů je poškozený.
89479014	Digitální podpis souboru neodpovídá digitálnímu podpisu společnosti Kaspersky.
89479015	Nelze použít klíč pro nekomerční licenci jako klíč pro komerční licenci.
89479016	K použití verze beta aplikace je vyžadována licence beta.
89479017	Soubor klíče není kompatibilní s touto aplikací.
89479018	Klíč je blokován společností Kaspersky.
89479019	Aplikace již byla použita na základě zkušební licence. Zkušební klíč nelze znovu přidat.
8947901A	Soubor klíče je poškozen.
8947901B	Digitální podpis chybí, je poškozen nebo neodpovídá digitálnímu podpisu společnosti Kaspersky.
8947901C	Nelze přidat klíč, pokud platnost příslušné nekomerční licence vypršela.
8947901E	Datum vytvoření nebo použití souboru klíče je neplatné. Zkontrolujte datum systému.
8947901F	Nelze přidat klíč pro zkušební licenci: je již aktivní jiný klíč pro zkušební licenci.
89479020	Seznam zakázaných klíčů je poškozený nebo chybí.
89479021	Popis aktualizace chybí nebo je poškozen.
89479022	Chyba v datech služby licenčního klíče.
89479023	Pro přidání rezervního klíče nelze použít neplatný soubor klíče.

89479025	Při odesílání požadavku na aktivační server došlo k chybě. Možné důvody: Chyba připojení k internetu nebo dočasné problémy na aktivačním serveru. Zkuste aplikaci později aktivovat pomocí aktivačního kódu. Pokud tato chyba přetrvává, kontaktujte svého poskytovatele internetu.
89479026	Chyba v odpovědi aktivačního serveru.
89479027	Nelze získat stav odpovědi.
89479028	Při ukládání dočasného souboru došlo k chybě.
89479029	Aktivační kód byl zadán nesprávně nebo je nesprávné systémové datum. Zkontrolujte systémové datum v počítači.
8947902A	Soubor klíče není kompatibilní s touto aplikací nebo platnost licence vypršela. Aplikaci Kaspersky Endpoint Security nemůžete aktivovat pomocí souboru klíčů pro jinou aplikaci.
8947902B	Nepodařilo se získat soubor klíče. Byl zadán nesprávný aktivační kód.
8947902C	Aktivační server vrátil chybu 400.
8947902D	Aktivační server vrátil chybu 401.
8947902E	Aktivační server vrátil chybu 403.
8947902F	Aktivační server vrátil chybu 404.
89479030	Aktivační server vrátil chybu 405.
89479031	Aktivační server vrátil chybu 406.
89479032	Je vyžadováno ověření na proxy serveru. Zkontrolujte nastavení sítě.
89479033	Časový limit požadavku vypršel.
89479034	Aktivační server vrátil chybu 409.
89479035	Aktivační server vrátil chybu 410.
89479036	Aktivační server vrátil chybu 411.
89479037	Aktivační server vrátil chybu 412.
89479038	Aktivační server vrátil chybu 413.
89479039	Aktivační server vrátil chybu 414.
8947903A	Aktivační server vrátil chybu 415.
8947903C	Interní chyba serveru.
8947903D	Funkce není podporována.
8947903E	Neplatná odpověď z brány. Zkontrolujte nastavení sítě.
8947903F	Služba není k dispozici (chyba HTTP 503).
89479040	Časový limit odezvy brány vypršel. Zkontrolujte nastavení sítě.
89479041	Tento protokol není serverem podporován.
89479043	Neznámá chyba HTTP.
89479044	Neplatné ID zdroje.
89479046	Neplatná adresa URL.
89479047	Neplatná cílová složka.
89479048	Chyba přidělení paměti.

89479049	Chyba při převodu parametrů na řetězec ANSI (URL, složka, agent).
8947904A	Chyba při vytváření pracovního vlákna.
8947904B	Pracovní vlákno je již spuštěno.
8947904C	Pracovní vlákno není spuštěno.
8947904D	Soubor klíčů nebyl na aktivačním serveru nalezen.
8947904E	Klíč je zablokován.
8947904F	Interní chyba aktivačního serveru.
89479050	V žádosti o aktivaci není dostatek údajů.
89479053	Platnost licenčního klíče vypršela.
89479054	V počítači je nastaveno nesprávné systémové datum.
89479055	Platnost zkušební licence vypršela.
89479056	Platnost licence vypršela.
89479057	Pro zadaný kód byl překročen limit počtu aktivací aplikace.
89479058	Postup aktivace byl ukončen systémovou chybou.
89479059	Nelze použít klíč pro nekomerční licenci jako klíč pro komerční licenci.
8947905C	Je vyžadován aktivační kód.
89479062	Nelze se připojit k aktivačnímu serveru.
89479064	Aktivační server není k dispozici. Zkontrolujte nastavení internetového připojení a opakujte aktivaci.
89479065	Datum vydání databáze aplikace je pozdější než datum vypršení licence.
89479066	Nelze nahradit aktivní klíč klíčem, jehož platnost vypršela.
89479067	Nelze přidat rezervní klíč, pokud jeho platnost vyprší před aktuální licencí.
89479068	Chybí aktualizovaný klíč předplatného.
8947906A	Nesprávný aktivační kód (kontrolní součet se neshoduje).
8947906B	Klíč je již aktivní.
8947906C	Typy licencí, které odpovídají aktivním a rezervním klíčům, se neshodují.
8947906D	Součást není licencí podporována.
8947906E	Tento klíč nelze přidat jako rezervní klíč.
89479213	Obecná chyba transportní vrstvy.
89479214	Nepodařilo se připojit k aktivačnímu serveru.
89479215	Neplatný formát adresy URL.
89479216	Nepodařilo se převést adresu proxy serveru.
89479217	Nepodařilo se převést adresu serveru. Zkontrolujte nastavení internetového připojení.
89479218	Nepodařilo se připojit k aktivačnímu serveru nebo proxy server.
89479219	Vzdálený přístup byl odepřen.
8947921A	Časový limit odezvy vypršel.

8947921B	Při odesílání požadavku HTTP došlo k chybě.
8947921C	Chyba připojení SSL.
8947921D	Operace byla přerušena zpětným hovorem.
8947921E	Příliš mnoho pokusů o přesměrování.
8947921F	Kontrola příjemce se nezdařila.
89479220	Prázdná odpověď z aktivačního serveru.
89479221	Při odesílání dat došlo k chybě.
89479222	Chyba při přijímání dat.
89479223	Místní chyba certifikátu SSL.
89479224	Chyba šifrování SSL.
89479225	Chyba certifikátu SSL serveru.
89479226	Neplatný obsah síťového paketu.
89479227	Přístup byl uživateli odepřen.
89479228	Neplatný soubor certifikátu SSL.
89479229	Nepodařilo se navázat připojení SSL.
8947922A	Nepodařilo se odeslat nebo přijmout síťový paket. Zkuste to znovu později.
8947922B	Neplatný soubor se zrušenými certifikáty.
8947922C	Chyba žádosti o certifikát SSL.
89479401	Neznámá chyba serveru.
89479402	Interní chyba serveru.
89479403	Pro zadaný aktivační kód není k dispozici žádný licenční klíč.
89479404	Aktivní klíč je zablokován.
89479405	Chybí požadované parametry žádosti o aktivaci aplikace.
89479406	Nesprávné uživatelské jméno nebo heslo.
89479407	Na server byl odeslán nesprávný aktivační kód.
89479408	Aktivační kód je pro aplikaci Kaspersky Endpoint Security neplatný. Aplikaci Kaspersky Endpoint Security nemůžete aktivovat pomocí souboru klíčů pro neznámou aplikaci.
89479409	V požadavku chybí aktivační kód.
8947940B	Platnost licence vypršela (podle údajů z aktivačního serveru).
8947940C	Byl překročen počet aktivací pomocí tohoto kódu.
8947940D	Neplatný formát ID požadavku.
8947940E	Aktivační kód je pro aplikaci Kaspersky Endpoint Security neplatný. Aktivační kód je určen pro jinou aplikaci společnosti Kaspersky.
8947940F	Licenční klíč nelze aktualizovat.
89479410	Aktivační kód je pro tuto oblast neplatný.
89479411	Aktivační kód je pro tuto jazykovou verzi aplikace Kaspersky Endpoint Security neplatný.

89479412	Je vyžadován další přístup k aktivačnímu serveru.
89479413	Aktivační server vrátil chybu 643.
89479414	Aktivační server vrátil chybu 644.
89479415	Aktivační server vrátil chybu 645.
89479416	Aktivační server vrátil chybu 646.
89479417	Aktivační server nepodporuje formát aktivačního kódu.
89479418	Neplatný formát aktivačního kódu.
89479419	V počítači je nastaven nesprávný systémový čas.
8947941A	Aktivační kód je pro tuto verzi aplikace Kaspersky Endpoint Security neplatný.
8947941B	Platnost předplatného vypršela.
8947941C	U tohoto licenčního klíče byl překročen počet aktivací.
8947941D	Neplatný digitální podpis licenčního klíče.
8947941E	Jsou zapotřebí další údaje.
8947941F	Ověření údajů uživatele se nezdařilo.
89479420	Předplatné je neaktivní.
89479421	Na aktivačním serveru probíhá údržba.
89479501	Neznámá chyba aplikace Kaspersky Endpoint Security.
89479502	Byl přenesen neplatný parametr (například prázdný seznam adres aktivačního serveru).
89479503	Nesprávný aktivační kód.
89479504	Neplatné uživatelské jméno.
89479505	Neplatné uživatelské heslo.
89479506	Neplatná odpověď z aktivačního serveru.
89479507	Žádost o aktivaci byla přerušena.
89479509	Aktivační server vrátil prázdný seznam pro přesměrování.

Příloha Profily aplikací

Profil je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Profily se používají ke správě aplikace z příkazového řádku. Pomocí profilů můžete provádět příkazy `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` a `IMPORT`. Pomocí profilů můžete konfigurovat nastavení aplikace (například `STOP DeviceControl`) nebo spouštět úlohy (například `START Scan_My_Computer`).

K dispozici jsou následující profily:

- `AdaptiveAnomaliesControl` – Adaptivní kontrola anomálií.
- `AMSI` – Ochrana AMSI.
- `BehaviorDetection` – Detekce chování.

- `DeviceControl` – Kontrola zařízení.
- `EntAppControl` – Kontrola aplikací.
- `File_Monitoring` nebo `FM` – Ochrana před souborovými hrozbami.
- `Firewall` nebo `FW` – Firewall.
- `HIPS` – Prevence narušení hostitele.
- `IDS` – Ochrana před síťovými hrozbami.
- `IntegrityCheck` – Kontrola integrity.
- `Mail_Monitoring` nebo `EM` – Ochrana před hrozbami v poště.
- `Rollback` – aktualizace vrácení.
- `Scan_ContextScan` – Kontrola z místní nabídky.
- `Scan_IdleScan` – Kontrola na pozadí.
- `Scan_Memory` – Prohledávání paměti jádra.
- `Scan_My_Computer` – Úplná kontrola.
- `Scan_Objects` – Vlastní kontrola.
- `Scan_Qscan` – Kontrola objektů, které se načítají při spouštění operačního systému.
- `Scan_Removable_Drive` – Kontrola vyměnitelných jednotek.
- `Scan_Startup` nebo `STARTUP` – Kontrola kritických oblastí.
- `Updater` – Aktualizace.
- `Web_Monitoring` nebo `WM` – Ochrana před webovými hrozbami.
- `WebControl` – Kontrola webu.

Aplikace Kaspersky Endpoint Security také podporuje profily služeb. Profily služeb mohou být vyžadovány při kontaktování technické podpory společnosti Kaspersky.

Správa aplikace prostřednictvím rozhraní REST API

Aplikace Kaspersky Endpoint Security umožňuje konfigurovat nastavení aplikace, spouštět prověřování, aktualizovat antivirové databáze a provádět další úkoly pomocí řešení třetích stran. Aplikace Kaspersky Endpoint Security poskytuje k těmto účelům rozhraní API. Rozhraní API Kaspersky Endpoint Security REST pracuje prostřednictvím protokolu HTTP a skládá se ze souboru metod požadavku/odpovědi. Jinými slovy můžete aplikaci Kaspersky Endpoint Security spravovat prostřednictvím řešení třetí strany, nikoli prostřednictvím místního aplikačního rozhraní nebo konzoly pro správu Kaspersky Security Center.

Chcete-li začít používat rozhraní REST API, musíte nainstalovat aplikaci Kaspersky Endpoint Security s podporou rozhraní REST API. Klient REST a Kaspersky Endpoint Security musí být nainstalovány ve stejném počítači.

Chcete-li zajistit bezpečnou interakci mezi aplikací Kaspersky Endpoint Security a klientem REST:

- Nakonfigurujte ochranu klienta REST před neoprávněným přístupem podle doporučení vývojáře klienta REST. Nakonfigurujte ochranu složky klienta REST před zápisem pomocí seznamu DACL.
- Pro spuštění klienta REST použijte zvláštní účet s oprávněními správci. Zakažte interaktivní přihlašování k systému pro tento účet.

Aplikace je spravována pomocí rozhraní REST API na adrese http://127.0.0.1 nebo http://localhost. Aplikaci Kaspersky Endpoint Security nelze spravovat vzdáleně pomocí rozhraní REST API.

OTEVŘÍT DOKUMENTACI ROZHRANÍ REST API

Instalace aplikace pomocí rozhraní REST API

Chcete-li spravovat aplikaci prostřednictvím REST API, musíte aplikaci Kaspersky Endpoint Security nainstalovat s podporou rozhraní REST API. Pokud spravujete aplikaci Kaspersky Endpoint Security pomocí rozhraní REST API, nemůžete aplikaci spravovat pomocí aplikace Kaspersky Security Center.

Instalace aplikace Kaspersky Endpoint Security s podporou rozhraní REST API:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, která obsahuje distribuční balíček aplikace Kaspersky Endpoint Security verze 11.2.0 nebo novější.
3. Nainstalujte aplikaci Kaspersky Endpoint Security s následujícím nastavením:
   - `RESTAPI=1`
   - `RESTAPI_User=<uživatelské jméno>`

     Uživatelské jméno pro správu aplikace pomocí rozhraní REST API. Zadejte uživatelské jméno ve formátu `<DOMAIN>\<UserName>` (například `RESTAPI_User=COMPANY\Administrator`). Aplikaci můžete spravovat prostřednictvím rozhraní REST API pouze pod tímto účtem. Pro práci s rozhraním REST API můžete vybrat pouze jednoho uživatele.
   - `RESTAPI_Port=<port>`

     Port používaný pro výměnu dat. Volitelný parametr. Ve výchozím nastavení je vybrán port 6782.
   - `AdminKitConnector=1`

Správa aplikací pomocí systémů pro správu. Ve výchozím nastavení je správa povolena.

Soubor setup.ini můžete také použít k definování nastavení pro práci s rozhraním REST API.

Nastavení pro práci s rozhraním REST API můžete definovat pouze během instalace aplikace. Po instalaci aplikace není možné nastavení změnit. Pokud chcete nastavení změnit, odinstalujte aplikaci Kaspersky Endpoint Security a znovu ji nainstalujte s novým nastavením pro práci s rozhraním REST API.

Příklad:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator /s
```

Díky tomu budete moci spravovat aplikaci pomocí rozhraní REST API. Chcete-li ověřit jeho fungování, otevřete dokumentaci rozhraní REST API pomocí požadavku GET.

Příklad:

```
GET http://localhost:6782/kes/v1/api-docs
```

Práce s API

Přístup k aplikaci prostřednictvím rozhraní REST API nelze omezit pomocí ochrany heslem. Není například možné uživateli zabránit v deaktivaci ochrany prostřednictvím rozhraní REST API. Ochranu heslem můžete nakonfigurovat pomocí rozhraní REST API a omezit přístup uživatelů k aplikaci prostřednictvím místního rozhraní.

Chcete-li spravovat aplikaci prostřednictvím rozhraní REST API, musíte spustit klienta REST pod účtem, který jste zadali při instalaci aplikace s podporou rozhraní REST API. Pro práci s rozhraním REST API můžete vybrat pouze jednoho uživatele.

OTEVŘÍT DOKUMENTACI ROZHRANÍ REST API

Správa aplikace prostřednictvím rozhraní REST API se skládá z následujících kroků:

1. Získejte aktuální hodnoty nastavení aplikace. Za tímto účelem odešlete požadavek GET.

   Příklad:

   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Aplikace odešle odpověď se strukturou a hodnotami nastavení. Aplikace Kaspersky Endpoint Security podporuje formáty XML a JSON.

   Příklad:

   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Upravte nastavení zásad. Za tímto účelem odešlete požadavek POST. Použijte strukturu nastavení přijatou v odpovědi na požadavek GET.

Příklad:

```
POST http://localhost:6782/kes/v1/settings/ExploitPrevention
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Aplikace použije změny v nastavení a odešle odpověď obsahující výsledky konfigurace aplikace.

Zdroje informací o aplikaci

Stránka aplikace Kaspersky Endpoint Security na webu společnosti Kaspersky

Na stránce aplikace Kaspersky Endpoint Security můžete zobrazit obecné informace o aplikaci a jejích funkcích.

Stránka aplikace Kaspersky Endpoint Security obsahuje odkaz na internetový obchod. Zde si můžete aplikaci zakoupit nebo obnovit.

Stránka aplikace Kaspersky Endpoint Security ve znalostní bázi

Znalostní báze je část na webu technické podpory.

Na stránce aplikace Kaspersky Endpoint Security ve znalostní bázi si můžete přečíst články, které poskytují užitečné informace, doporučení a odpovědi na časté dotazy týkající se nákupu, instalace a používání aplikace.

Články znalostní báze mohou odpovídat na otázky týkající se nejen aplikace Kaspersky Endpoint Security, ale také jiných aplikací společnosti Kaspersky. Články ve znalostní bázi mohou také obsahovat novinky od technické podpory.

Diskuse o aplikacích Kaspersky v komunitě uživatelů

Pokud vaše otázka nevyžaduje naléhavou odpověď, můžete ji prodiskutovat s odborníky společnosti Kaspersky a dalšími uživateli v naší komunitě.

V Komunitě si můžete prohlédnout stávající témata, psát komentáře a vytvářet nová diskusní témata.

Kontaktování technické podpory

Pokud řešení svého problému nenaleznete v dokumentaci aplikace nebo v jiném ze zdrojů informací o aplikaci Kaspersky Endpoint Security, doporučujeme vám obrátit se na technickou podporu. Odborníci technické podpory zodpoví vaše dotazy týkající se instalace a používání aplikace Kaspersky Endpoint Security.

Společnost Kaspersky poskytuje podporu pro aplikaci Kaspersky Endpoint Security během jejího životního cyklu (viz stránka životního cyklu aplikace). Dříve než se obrátíte na technickou podporu, přečtěte si prosím pravidla podpory.

Technickou podporu můžete kontaktovat jedním z těchto způsobů:

- Návštěva webu technické podpory
- Zasláním žádosti technické podpoře společnosti Kaspersky prostřednictvím portálu Kaspersky CompanyAccount.

Jakmile odborníky technické podpory společnosti Kaspersky informujete o svém problému, mohou vás vyzvat k vytvoření *souboru trasování*. Soubor trasování umožňuje trasování příkazů aplikace krok za krokem a určení fáze činnosti aplikace, v níž došlo k chybám.

Odborníci technické podpory mohou také vyžadovat další informace o operačním systému, procesech spuštěných v počítači a podrobných zprávách o provozu součástí aplikace.

Při provádění diagnostiky vás mohou odborníci technické podpory vyzvat ke změně nastavení aplikace:

- aktivováním funkce, která přijímá rozšířené diagnostické informace;
- vyladěním nastavení jednotlivých součástí aplikace, které nejsou dostupné prostřednictvím standardních prvků uživatelského rozhraní;
- změnou nastavení ukládání diagnostických informací;
- konfigurací zachycování a protokolování síťového provozu.

Odborníci technické podpory vám poskytnou veškeré informace potřebné k vykonání těchto operací (popis jednotlivých kroků postupu, upravovaných nastavení, konfiguračních souborů, skriptů, dodatečných funkcí příkazového řádku, modulů ladění, specializovaných nástrojů apod.) a informují vás o rozsahu dat používaných pro účely ladění. Rozšířené diagnostické informace budou uloženy v počítači uživatele. Data nebudou automaticky odeslána společnosti Kaspersky.

Výše uvedené operace by měly být prováděny pouze pod dohledem odborníků technické podpory a na základě jejich pokynů. Provádění změn nastavení aplikace bez dohledu a způsobem, který neodpovídá postupům v příručce pro správce nebo pokynům odborníků technické podpory, může zpomalit operační systém nebo způsobit jeho zhroucení, ovlivnit zabezpečení počítače nebo ohrozit dostupnost či integritu zpracovávaných dat.

Obsah a uložení souborů trasování

Uživatel je osobně odpovědný za zabezpečení dat, která jsou uložena v jeho počítači, především za sledování a omezení přístupu k datům, dokud nejsou odeslána společnosti Kaspersky.

Soubory trasování jsou ukládány do počítače za předpokladu, že je aplikace používána. Po odebrání aplikace jsou soubory trvale odstraněny.

Soubory trasování, kromě souborů trasování ověřovacího agenta, jsou uloženy ve složce% ProgramData%\Kaspersky Lab\KES\Traces.

Soubory trasování jsou pojmenovány takto: `KES<číslo verze služby_datumXX.XX_čas.XX_pidXXX.><typ souboru trasování>.log`.

Data uložená v souboru trasování si můžete prohlédnout.

Všechny soubory trasování obsahují následující běžná data:

- čas události;
- počet vláken provádění;

  soubor trasování ověřovacího agenta tyto informace neobsahuje;

- součást aplikace, která událost způsobila;
- stupeň závažnosti události (informační událost, varování, kritická událost, chyba);
- popis události zahrnující vykonání příkazu součástí aplikace a výsledek vykonání tohoto příkazu.

Aplikace Kaspersky Endpoint Security ukládá uživatelská hesla do souboru trasování pouze v šifrované podobě.

Obsah souborů trasování SRV.log, GUI.log a ALL.log

V souborech trasování `SRV.log`, `GUI.log` a `ALL.log` se mohou kromě obecných dat ukládat následující informace:

- Osobní data, včetně příjmení, křestního jména a druhého jména, pokud jsou takové údaje součástí cesty k souborům v místním počítači.
- Data na hardwaru nainstalovaném v počítači (například data firmwaru BIOS/UEFI). Tato data se zapisují do trasovacího souboru při provádění funkce Kaspersky Disk Encryption.
- Uživatelské jméno a heslo v případě, že tyto údaje byly odesílány otevřeně. Tato data lze zaznamenat v souborech trasování během kontroly internetového provozu.
- Uživatelské jméno a heslo v případě, že jsou tyto údaje v hlavičkách protokolu HTTP.
- Název účtu v systému Microsoft Windows, pokud je název účtu součástí názvu souboru.
- Vaše e-mailová adresa nebo webová adresa obsahující název účtu a heslo, jestliže jsou tyto údaje součástí názvu zjištěného objektu.

- Vámi navštívené webové stránky a přesměrování z těchto webových stránek. Tato data jsou zapisována do souborů trasování, když aplikace kontroluje webové stránky.
- Adresa proxy serveru, název počítače, port, IP adresa a uživatelské jméno používané k přihlášení k proxy serveru. Tato data jsou zapisována do souborů trasování, jestliže aplikace používá nějaký proxy server.
- Vzdálené IP adresy, k nimž se váš počítač připojuje.
- Předmět zprávy, ID, jméno odesílatele a adresa webové stránky odesílatele zprávy v sociální síti. Tato data jsou zapisována do souborů trasování, jestliže je povolena součást Kontrola webu.
- Data týkající se síťového provozu. Tato data se zapisují do trasovacích souborů, pokud jsou povoleny součásti pro sledování provozu (například Kontrola webu).
- Data přijatá ze serverů Kaspersky (například verze antivirových databází).
- Stavy součástí aplikace Kaspersky Endpoint Security a jejich provozní data.
- Data o činnosti uživatele v aplikaci.
- Události operačního systému.

Obsah souborů trasování HST.log, BL.log, Dumpwriter.log, WD.log a AVPCon.dll.log

V souboru trasování `HST.log` jsou kromě obecných dat také informace o vykonání úloh aktualizace databází a modulů aplikací.

V souboru trasování `BL.log jsou` kromě obecných dat také informace o událostech, k nimž došlo během použití aplikace, a také data nutná k řešení potíží spojených s chybami aplikace. Tento soubor se vytvoří, pokud je aplikace spuštěna s parametrem avp.exe –bl.

V souboru trasování `Dumpwriter.log` jsou kromě obecných dat také informace o službách potřebné k řešení chyb, k nimž dojde při vytváření souboru výpisu aplikace.

V souboru trasování `WD.log` jsou kromě obecných dat také informace o událostech, k nimž došlo během použití služby avpsus, včetně událostí aktualizace modulů aplikace.

V souboru trasování `AVPCon.dll.log` jsou kromě obecných dat také informace o událostech, k nimž došlo během použití modulu pro připojení aplikace Kaspersky Security Center.

Obsah souborů trasování výkonu

Soubory trasování výkonu jsou pojmenovány následovně: `KES<číslo verze_datumXX.XX_časXX.XX_pidXXX.> PERF.HAND.etl`.

Soubory trasování výkonu obsahují kromě obecných dat informace o zatížení procesoru, informace o době načítání operačního systému a aplikací a informace o spuštěných procesech.

Obsah souboru trasování součásti Ochrana AMSI

Vedle obecných dat obsahuje soubor trasování AMSI.log informace o výsledcích kontrol provedených na základě požadavků od aplikací třetích stran.

Obsah souborů trasování součásti Ochrana před hrozbami v poště

Soubor trasování `mcou.OUTLOOK.EXE.log` může vedle obecných dat obsahovat části e-mailových zpráv, včetně e-mailových adres.

Obsah souborů trasování součásti Kontrola z místní nabídky

Soubor trasování `shellex.dll.log` obsahuje vedle obecných informací informace o dokončení úlohy kontroly a data vyžadovaná k ladění aplikace.

Obsah souborů trasování webového modulu plug-in aplikace

Soubory trasování webového modulu plug-in aplikace jsou uloženy v počítači, ve kterém je nasazena Kaspersky Security Center 12 Web Console, a to ve složce Program Files\Kaspersky Lab\Kaspersky Security Center Web Console 12\logs.

Soubory trasování webového modulu plug-in aplikace jsou pojmenovány následujícím způsobem: `logs-kes_windows-<typ souboru trasování>.DESKTOP-<datum aktualizace souboru>.log`. Webová konzole začne po instalaci zapisovat data a po odebrání webové konzole soubory trasování odstraní.

V souborech trasování webového modulu plug-in aplikace se mohou kromě obecných dat ukládat následující informace:

- heslo uživatele KLAdmin k odemknutí rozhraní aplikace Kaspersky Endpoint Security (ochrana heslem),
- dočasné heslo k odemknutí rozhraní aplikace Kaspersky Endpoint Security (ochrana heslem),
- uživatelské jméno a heslo poštovního serveru SMTP (e-mailová upozornění),
- uživatelské jméno a heslo internetového proxy serveru (proxy server),
- uživatelské jméno a heslo k úloze *Změnit součásti aplikace*,
- přihlašovací údaje k účtům a cesty uvedené v úlohách a vlastnostech zásad aplikace Kaspersky Endpoint Security.

Obsah souboru trasování ověřovacího agenta

Soubor trasování ověřovacího agenta je ukládán do složky s informacemi o systémovém svazku a má tento název: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

V souboru trasování ověřovacího agenta jsou kromě obecných dat také informace o provozu ověřovacího agenta a akcích uživatele provedených s ověřovacím agentem.

Trasování aplikací

Trasování aplikací jsou podrobné záznamy o akcích, které aplikace provedla, a o zprávách o událostech, ke kterým došlo během provozu aplikace.

Trasování aplikací by mělo být prováděno pod dohledem technické podpory společnosti Kaspersky.

Postup vytvoření souboru trasování aplikace:

1. V hlavním okně aplikace klikněte na tlačítko .

   Otevře se okno **Podpora**.

2. V okně **Podpora** klikněte na tlačítko **Podpůrné nástroje**.

3. Pomocí přepínače **Povolit trasování aplikace** můžete povolit nebo zakázat trasování provozu aplikace.

4. V rozevíracím seznamu **Trasování** vyberte režim trasování aplikací:

   - **se střídáním**. Uloží trasování do omezeného počtu souborů s omezenou velikostí; když je dosaženo maximální velikosti, přepíše starší soubory. Pokud je vybrán tento režim, můžete definovat maximální počet souborů pro střídání a maximální velikost pro každý soubor.

   - **Zápis do 1 souboru**. Uloží jeden soubor trasování (bez omezení velikosti).

5. V rozevíracím seznamu **Úroveň** vyberte úroveň trasování.

   O požadované úrovni trasování se poraďte s odborníkem technické podpory. Pokud asistence technické podpory není k dispozici, nastavte úroveň trasování na možnost **Normální (500)**.

6. Restartujte aplikaci Kaspersky Endpoint Security.

7. Chcete-li zastavit proces trasování, vraťte se do okna **Podpora** a deaktivujte trasování.

Soubory trasování můžete také vytvořit při instalaci aplikace z příkazového řádku, včetně použití souboru setup.ini.

Soubory trasování jsou ukládány do počítače za předpokladu, že je aplikace používána. Po odebrání aplikace jsou soubory trvale odstraněny. Soubory trasování, kromě souborů trasování ověřovacího agenta, jsou uloženy ve složce% ProgramData%\Kaspersky Lab\KES\Traces. Ve výchozím nastavení je trasování zakázáno.

Trasování výkonu aplikace

Aplikace Kaspersky Endpoint Security umožňuje přijímat informace o problémech s provozem počítače během používání aplikace. Můžete například obdržet informace o zpoždění při načítání operačního systému po instalaci aplikace. Za tímto účelem aplikace Kaspersky Endpoint Security vytváří soubory trasování výkonu. *Trasování výkonu* znamená protokolování akcí prováděných aplikací za účelem diagnostiky problémů s výkonem u aplikace Kaspersky Endpoint Security. K získání informací používá aplikace Kaspersky Endpoint Security službu Trasování událostí pro Windows (ETW). Technická podpora společnosti Kaspersky odpovídá za diagnostiku problémů aplikace Kaspersky Endpoint Security a zjištění důvodů těchto problémů.

Trasování aplikací by mělo být prováděno pod dohledem technické podpory společnosti Kaspersky.

Postup vytvoření souboru trasování výkonu:

1. V hlavním okně aplikace klikněte na tlačítko .

   Otevře se okno **Podpora**.

2. V okně **Podpora** klikněte na tlačítko **Podpůrné nástroje**.

3. Pomocí přepínače **Povolit trasování výkonu** můžete povolit nebo zakázat trasování výkonu aplikace.

4. V rozevíracím seznamu **Trasování** vyberte režim trasování aplikací:

   - **se střídáním**. Uloží trasování do omezeného počtu souborů s omezenou velikostí; když je dosaženo maximální velikosti, přepíše starší soubory. Pokud je vybrán tento režim, můžete definovat maximální velikost pro každý soubor.

   - **Zápis do 1 souboru**. Uloží jeden soubor trasování (bez omezení velikosti).

5. V rozevíracím seznamu **Úroveň** vyberte úroveň trasování:

   - **Lehké**. Kaspersky Endpoint Security analyzuje hlavní procesy operačního systému související s výkonem.

   - **Podrobné.** Kaspersky Endpoint Security analyzuje všechny procesy operačního systému související s výkonem.

6. V rozevíracím seznamu **Typ trasování** vyberte typ trasování:

   - **Základní informace**. Kaspersky Endpoint Security analyzuje procesy, když je spuštěn operační systém. Tento typ trasování použijte, pokud problém přetrvává po načtení operačního systému, například problém s přístupem k internetu v prohlížeči.

   - **Při restartu**. Kaspersky Endpoint Security analyzuje procesy, pouze když je spuštěn operační systém. Po načtení operačního systému aplikace Kaspersky Endpoint Security trasování zastaví. Tento typ trasování použijte, pokud problém souvisí se zpožděným načítáním operačního systému.

7. Restartujte počítač a pokuste se problém reprodukovat.

8. Chcete-li zastavit proces trasování, vraťte se do okna **Podpora** a deaktivujte trasování.

Soubor trasování výkonu se vytvoří ve složce %ProgramData%\Kaspersky Lab\KES\Traces. Po vytvoření souboru trasování odešlete soubor Technical Support společnosti Kaspersky.

Zápis souborů výpisu

Soubor výpisu obsahuje všechny informace o pracovní paměti procesů aplikace Kaspersky Endpoint Security v okamžiku vytvoření souboru výpisu.

Uložené soubory výpisu mohou obsahovat důvěrná data. Chcete-li regulovat přístup ke svým datům, je nutné nezávisle zajistit zabezpečení souborů výpisu.

Soubory výpisu jsou ukládány do počítače za předpokladu, že je aplikace používána. Po odebrání aplikace jsou soubory trvale odstraněny. Soubory výpisu se ukládají ve složce %ProgramData%\Kaspersky Lab\KES\Traces.

Postup povolení nebo zakázání zápisu výpisu paměti:

1. V dolní části okna aplikace klikněte na tlačítko ⚙.

2. V okně s nastavením aplikace vyberte část **Obecné**.

3. V bloku **Informace o ladění** pomocí zaškrtávacího políčka **Povolit zápis výpisu paměti** povolte nebo zakažte zápis výpisu paměti aplikace.

4. Uložte změny.

Ochrana souborů výpisu a trasovacích souborů

Soubory výpisu a trasování obsahují informace o operačním systému a mohou také obsahovat uživatelská data. Aby nemohlo dojít k neoprávněnému přístupu k těmto informacím, můžete aktivovat ochranu souborů výpisu a trasování.

Pokud je ochrana souborů výpisu a trasování povolena, k souborům budou mít přístup následující uživatelé:

- K souborům výpisu má přístup správce systému, místní správce a uživatel, který zápis těchto souborů výpisu a trasování povolil.
- K souborům trasování má přístup pouze správce systému a místní správce.

Postup povolení nebo zakázání ochrany souborů výpisu a trasování:

1. V dolní části okna aplikace klikněte na tlačítko .

2. V okně s nastavením aplikace vyberte část **Obecné**.

3. V bloku **Informace o ladění** povolte nebo zakažte ochranu souborů pomocí zaškrtávacího políčka **Povolit ochranu souborů výpisu a trasování**.

4. Uložte změny.

Soubory výpisu a trasování zapsané během období, kdy byla ochrana aktivní, zůstanou chráněny i po deaktivaci této funkce.

Omezení a varování

Aplikace Kaspersky Endpoint Security má řadu omezení, která nejsou pro provoz aplikace významná.

Instalace aplikace

- Podrobnosti o podpoře operačních systémů Microsoft Windows 10, Microsoft Windows Server 2016 a Microsoft Windows Server 2019 najdete ve znalostní bázi technické podpory.

- Po instalaci do infikovaného počítače aplikace neinformuje uživatele o nutnosti spustit kontrolu počítače. Při aktivaci aplikace se mohou vyskytnout problémy. Chcete-li tyto problémy vyřešit, spusťte kontrolu kritických oblastí.

- Pokud jsou v souborech setup.ini a setup.reg použity jiné znaky než ASCII (například písmena v azbuce), doporučujeme soubor upravit pomocí programu notepad.exe a uložit jej v kódování UTF-16LE. Jiná kódování nejsou podporována.

- Aplikace nepodporuje při zadávání instalační cesty aplikace v nastavení instalačního balíčku jiné znaky než ASCII.

- Při importu nastavení aplikace ze souboru CFG se nepoužije hodnota nastavení, která definuje účast v aplikaci Kaspersky Security Network. Po importu nastavení si přečtěte text Prohlášení ke službě Kaspersky Security Network a potvrďte svůj souhlas s účastí v této službě. Text prohlášení si můžete přečíst v rozhraní aplikace nebo v souboru ksn_*.txt umístěném ve složce obsahující sadu pro distribuci aplikací.

- Při upgradu z aplikace Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 (sestavení 10.3.0.6294) je zapnuta součást Prevence narušení hostitele.

- Při aktualizaci aplikace Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 (sestavení 10.3.0.6294) budou soubory, které byly v předchozí verzi aplikace umístěny v záloze nebo karanténě, přesunuty v nové verzi aplikace do zálohy. Tyto soubory se nepřenášejí u verzí starších než Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 (sestavení 10.3.0.6294). Chcete-li je uložit, musíte před upgradem aplikace obnovit soubory z karantény a zálohy. Po dokončení upgradu obnovené soubory znovu zkontrolujte.

- Pokud chcete odebrat a znovu nainstalovat šifrování (FLE nebo FDE) nebo součást Kontrola zařízení, musíte před opětovnou instalací restartovat systém.

- Pokud používáte operační systém Microsoft Windows 10, musíte systém po odebrání součásti Šifrování na úrovni souborů (FLE) restartovat.

- Při pokusu o instalaci libovolné verze šifrovacího modulu AES do počítače, na němž je nainstalována aplikace Kaspersky Endpoint Security 11.6.0, ale nejsou nainstalovány žádné šifrovací součásti, bude instalace šifrovacího modulu ukončena chybovou zprávou, že je nainstalována novější verze aplikace. Počínaje aplikací Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 (verze 10.3.0.6294) neexistuje pro šifrovací modul samostatný instalační soubor. Šifrovací knihovny jsou součástí sady pro distribuční balíček aplikace. Aplikace Kaspersky Endpoint Security 11.6.0 je nekompatibilní s šifrovacími moduly AES. Knihovny potřebné pro šifrování se nainstalují automaticky, když je vybrána součást Úplné šifrování disku (FDE) nebo Šifrování na úrovni souborů (FLE).

- Instalace aplikace může skončit chybovým hlášením *V počítači je nainstalována aplikace, jejíž název chybí nebo je nečitelný*. To znamená, že ve vašem počítači zůstávají nekompatibilní aplikace nebo jejich fragmenty. Chcete-li odstranit artefakty nekompatibilních aplikací, odešlete požadavek s podrobným popisem situace technické podpoře společnosti Kaspersky prostřednictvím portálu Kaspersky CompanyAccount.

- Od verze aplikace 11.0.0 můžete modul plug-in konzoly pro správu aplikace Kaspersky Endpoint Security pro systém Windows instalovat přes předchozí verzi modulu plug-in. Pro návrat k předchozí verzi modulu plug-in odstraňte aktuální modul plug-in a nainstalujte předchozí verzi.

- Při upgradu aplikace Kaspersky Endpoint Security 11.0.0 nebo 11.0.1 pro systém Windows se nastavení místního plánu úloh pro úlohy *Aktualizace*, *Kontrola kritických oblastí*, *Vlastní kontrola* a *Kontrola integrity*

neuloží.

- Pokud jste zrušili odebrání aplikace, spusťte její obnovení po restartu počítače.
- V počítačích se systémem Windows 10 verze 1903 a 1909 může upgrade z aplikace Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 Maintenance Release 3 (sestavení 10.3.3.275), Service Pack 2 Maintenance Release 4 (sestavení 10.3.3.304), 11.0.0 a 11.0.1 s nainstalovanou součástí Šifrování na úrovni souborů (FLE) skončit chybou. Důvodem je, že šifrování souborů není u těchto verzí aplikace Kaspersky Endpoint Security pro systém Windows ve Windows 10 verze 1903 a 1909 podporováno. Před instalací této aktualizace se doporučuje odebrat součást šifrování souborů.
- Pokud upgradujete předchozí verzi aplikace na verzi 11.6.0 a chcete nainstalovat aplikaci Kaspersky Endpoint Agent, restartujte počítač a přihlaste se do systému pomocí účtu s právy místního správce. V opačném případě nebude aplikace Kaspersky Endpoint Agent během upgradu nainstalována.
- Pokud je aplikace neúspěšně nainstalována se součástí Kaspersky Endpoint Agent vybranou v operačním systému serveru a zobrazí se okno *Chyba koordinátoru instalačního programu systému Windows*, postupujte podle pokynů na webu podpory společnosti Microsoft.
- Pokud byla aplikace nainstalována místně v neinteraktivním režimu, použijte k nahrazení nainstalovaných součástí poskytnutý soubor setup.ini.
- Pokud upgradujete aplikaci Kaspersky Endpoint Security 10 pro systém Windows Service Pack 2 Maintenance Release 4 s nainstalovanou součástí Šifrování na úrovni souborů (FLE) v počítačích se systémem Windows 10 verze 1809, 1903 a 1909, do bitové kopie WinRe nebudou nainstalovány ovladače FDE.
- Po instalaci aplikace Kaspersky Endpoint Security pro systém Windows v některých konfiguracích systému Windows 7 bude program Windows Defender nadále fungovat. Doporučuje se ručně deaktivovat program Windows Defender, aby se zabránilo snížení výkonu systému.
- Po upgradu aplikace z verzí starších než Kaspersky Endpoint Security 11 pro Windows musí být počítač restartován.

Podpora serverových platforem

- Systém ReFS je podporován s určitými omezeními:
  - Po spuštění antivirové kontroly jsou výjimky z kontroly přidané pomocí nástroje iChecker resetovány při restartu serveru.
  - Pokud byl před instalací aplikace Kaspersky Endpoint Security v počítači přítomen soubor meicar.exe, aplikace nezjišťuje soubory eicar.com a susp-eicar.com.
- Není podporována konfigurace jádra serveru ani režimu clusteru.
- Na serverových platformách nejsou podporovány technologie Šifrování na úrovni souborů (FLE) ani Kaspersky Disk Encryption (FDE).
- Kontrola zařízení není podporována na serverových platformách.
- Z podpory byl vyřazen Microsoft Windows Server 2008. - Není podporována instalace aplikace v počítači s operačním systémem Microsoft Windows Server 2008.
- Pokud jste na terminálovém serveru zahájili několik pracovních relací, upozornění aplikace Kaspersky Endpoint Security nemusí fungovat správně. Příklad: uživatel relace č. 1 spustí kontrolu reputace souborů v KSN. Kaspersky Endpoint Security zobrazí upozornění s výsledkem kontroly uživateli relace č. 2.

Podpora virtuálních platforem

- Šifrování celého disku (FDE) na virtuálních strojích Hyper-V není podporováno.
- Šifrování celého disku (FDE) na virtuálních platformách Citrix není podporováno.
- Více relací v systému Windows 10 Enterprise je podporováno s omezeními:
  - Kaspersky Endpoint Security považuje více relací Windows 10 Enterprise za operační systém serveru. Více relací v systému Windows 10 Enterprise je podporováno s omezeními pro serverovou platformu. Například servery nemohou používat některé součásti aplikace Kaspersky Endpoint Security. Aplikace rovněž místo licenčního klíče pro pracovní stanici používá licenční klíč pro server.
  - Není podporováno úplné šifrování disku (FDE).
  - Není podporována správa nástroje BitLocker.
  - Není podporováno používání aplikace Kaspersky Endpoint Security s vyměnitelnými jednotkami. Infrastruktura Microsoft Azure definuje vyměnitelné jednotky jako síťové jednotky.
- Instalace a použití šifrování na úrovni souborů (FLE) na virtuálních platformách Citrix není podporováno.
- Chcete-li podporovat kompatibilitu aplikace Kaspersky Endpoint Security pro Windows s Citrix PVS, proveďte instalaci se zapnutou volbou **Zajistit kompatibilitu s Citrix PVS**. Tuto možnost lze povolit v průvodci instalací nebo pomocí parametru příkazového řádku `/pCITRIXCOMPATIBILITY=1`. V případě vzdálené instalace musí být soubor KUD upraven přidáním následujícího parametru: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. Chcete-li klonovat virtuální počítače, které používají vDisk, před zahájením klonování musíte deaktivovat sebeobranu.
- Při přípravě počítače-šablony pro hlavní bitovou kopii Citrix XenDesktop s předinstalovanou aplikací Kaspersky Endpoint Security pro systém Windows a Síťovým agentem aplikace Kaspersky Security Center přidejte do konfiguračního souboru následující typy výjimek:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Podrobnosti o nástroj Citrix XenDesktop najdete na webu podpory Citrix.
- V některých případech může být pokus o bezpečné odpojení vyměnitelné jednotky neúspěšný na virtuálním počítači, který je nasazen na hypervizoru VMware ESXi. Pokuste se zařízení znovu bezpečně odpojit.

Kompatibilita s aplikací Kaspersky Security Center

- Součást Adaptivní kontrola anomálií můžete spravovat pouze v aplikaci Kaspersky Security Center verze 11 nebo novější.
- Zpráva o ohrožení aplikace Kaspersky Security Center 11 nemusí zobrazovat informace o akcích provedených na hrozbách, které byly detekovány součástí Ochrana AMSI.
- Provozní stav součásti Ochrana AMSI a Adaptivní kontrola anomálií je k dispozici pouze v aplikaci Kaspersky Security Center verze 11 nebo novější. Provozní stav lze zobrazit v konzole pro správu aplikace Kaspersky Security Center ve vlastnostech počítače v části **Úlohy**. Zprávy pro tyto součásti jsou k dispozici rovněž v aplikaci Kaspersky Security Center verze 11 nebo novější.

Správa licence

- Pokud se zobrazí zpráva *Chyba přijímání dat*, ověřte, zda má počítač, na kterém provádíte aktivaci, přístup k síti, nebo nakonfigurujte nastavení aktivace pomocí aktivačního proxy serveru aplikace Kaspersky Security Center.
- Aplikaci nelze aktivovat předplatným prostřednictvím aplikace Kaspersky Security Center, pokud platnost licence vypršela nebo pokud je v počítači aktivní zkušební licence. Chcete-li nahradit zkušební licenci nebo licenci, jejíž platnost brzy vyprší, licencí předplatného, použijte úlohu distribuce licence.
- V rozhraní aplikace se datum vypršení platnosti licence zobrazuje v místním čase počítače.
- Instalace aplikace se souborem vloženého klíče do počítače, který má nestabilní přístup k internetu, může mít za následek dočasné zobrazení událostí, které uvádějí, že aplikace není aktivována nebo že licence neumožňuje činnost součásti. Důvodem je, že aplikace nejprve nainstaluje a pokusí se aktivovat vloženou zkušební licenci, která vyžaduje aktivaci přístupu k internetu během instalace.
- Během zkušebního období může instalace jakéhokoli upgradu nebo opravy aplikace v počítači, který má nestabilní přístup k internetu, vést k dočasnému zobrazení událostí, které uvádějí, že aplikace není aktivována. Důvodem je, že aplikace znovu nainstaluje a pokusí se aktivovat integrovanou zkušební licenci, která vyžaduje při instalaci upgradu aktivaci přístupu k internetu.
- Pokud byla zkušební licence automaticky aktivována během instalace aplikace a poté byla aplikace odebrána bez uložení licenčních údajů, aplikace se po opětovné instalaci automaticky neaktivuje se zkušební licencí. V takovém případě aplikaci aktivujte ručně.
- Pokud používáte aplikaci Kaspersky Security Center verze 11 a aplikaci Kaspersky Endpoint Security verze 11.6.0, zprávy o výkonu součásti nemusí fungovat správně. Jestliže jste si nainstalovali součásti aplikace Kaspersky Endpoint Security, které nejsou zahrnuty ve vaší licenci, Síťový agent může chyby stavu součásti odesílat do protokolu událostí systému Windows. Chcete-li předejít chybám, odeberte součásti, které nejsou zahrnuty ve vaší licenci.

Modul pro nápravu

- Aplikace obnoví soubory pouze v zařízeních se souborovým systémem NTFS nebo FAT32.
- Aplikace může obnovit soubory s následujícími příponami: ODT, ODS, ODP, ODM, ODC, ODB, DOC, DOCX, DOCM, WPS, XLS, XLSX, XLSM, XLSB, XLK, PPT, PPTX, PPTM, MDB, ACCDB, PST, DWG, DXF, DXG, WPD, RTF, WB2, PDF, MDF, DBF, PSD, PDD, EPS, AI, INDD, CDR, JPG, JPE, DNG, 3FR, ARW, SRF, SR2, BAY, CRW, CR2, DCR, KDC, RF, MEF, MRW, NEF, NRW, ORF, RAF, RAW, RWL, RW2, R3D, PTX, PEF, SRW, X3F, DER, CER, CRT, PEM, PFX, P12, P7B, P7C, 1CD.
- Soubory umístěné na síťových jednotkách nebo na přepisovatelných discích CD/DVD není možné obnovit.
- Soubory, které byly zašifrovány pomocí systému EFS (Encryption File System), není možné obnovit. Podrobnější informace o fungování systému EFS najdete na *webu společnosti Microsoft*.
- Aplikace nesleduje úpravy souborů provedené procesy na úrovni jádra operačního systému.
- Aplikace nesleduje úpravy souborů přes síťové rozhraní (například pokud je soubor uložen ve sdílené složce a proces je spuštěn vzdáleně z jiného počítače).

Brána firewall

- Filtrace paketů nebo připojení podle místní adresy, fyzického rozhraní a doby životnosti paketů (TTL) je podporována v následujících případech:
  - Podle místní adresy pro odchozí pakety nebo připojení v pravidlech aplikace pro TCP a UDP a pravidla paketů.
  - Podle místní adresy pro příchozí pakety nebo připojení (kromě UDP) v pravidlech blokování aplikace a pravidlech paketů.
  - Podle doby životnosti paketů (TTL) v pravidlech blokových paketů pro příchozí nebo odchozí pakety.
  - Podle síťového rozhraní pro příchozí a odchozí pakety nebo připojení v pravidlech paketů.
- Ve verzích aplikací 11.0.0 a 11.0.1 jsou definované adresy MAC použity nesprávně. Nastavení adresy MAC pro verze 11.0.0, 11.0.1 a 11.1.0 nebo novější není kompatibilní. Po upgradu aplikace nebo pluginu z těchto verzí na verzi 11.1.0 nebo novější musíte ověřit a překonfigurovat definované adresy MAC v pravidlech brány firewall.
- Při upgradu aplikace z verze 11.1.1 a 11.2.0 na verzi 11.6.0 nebudou migrovány stavy oprávnění pro následující pravidla brány firewall:
  - Požadavky na server DNS přes protokol TCP.
  - Požadavky na server DNS přes protokol UDP.
  - Jakákoli síťová aktivita.
  - Příchozí reakce na zprávu ICMP Cíl nedostupný.
  - Příchozí datový proud ICMP.
- Pokud jste nakonfigurovali síťový adaptér nebo dobu životnosti paketu (TTL) pro povolující pravidlo paketu, je priorita tohoto pravidla nižší než blokující pravidlo aplikace. Jinými slovy, pokud je pro aplikaci blokována síťová aktivita (například aplikace je ve skupině důvěryhodnosti *Vysoké omezení*), nemůžete povolit síťovou aktivitu aplikace pomocí pravidla paketu s tímto nastavením. Ve všech ostatních případech je priorita pravidla paketu vyšší než pravidlo sítě aplikace.
- V aplikaci Kaspersky Endpoint Security pro systém Windows 11.5.0–11.6.0 může při importu seznamu pravidel paketů brány firewall dojít k chybě. To může vést k odstranění uživatelem definovaných místních nebo vzdálených adres z pravidla. Chcete-li tuto chybu opravit, kontaktujte technickou podporu. Technická podpora vám poskytne bezpečnostní opravu pro tento plugin. Případně můžete po vydání nové verze upgradovat aplikaci na tuto verzi.
- Při importu pravidel paketů brány firewall může aplikace Kaspersky Endpoint Security změnit názvy pravidel. Aplikace identifikuje pravidla, která mají stejnou sadu hlavních parametru, například protokol, směr, vzdálené a místní porty a dobu životnosti paketu (TTL). Pokud je tato sada hlavních parametrů u více pravidel stejná, aplikace těmto pravidlům přiřadí stejný název nebo přidá k názvu značku parametru. To znamená, že aplikace Kaspersky Endpoint Security importuje všechna pravidla paketů, ale názvy pravidel, která mají stejné hlavní parametry, se mohou změnit.
- Když je v aplikaci Kaspersky Endpoint Security 11.6.0 nebo dřívější aktivováno pravidlo síťových paketů, ve sloupci **Název aplikace** ve zprávě brány firewall se vždy bude zobrazovat hodnota *Kaspersky Endpoint Security*. Kromě toho bude brána firewall blokovat připojení na úrovni paketů pro všechny aplikace. Toto chování se změnilo u aplikace Kaspersky Endpoint Security 11.7.0 a pozdější. Do zprávy brány firewall byl přidán sloupec **Typ pravidla**. Po aktivaci pravidla síťových paketů hodnota ve sloupci **Název aplikace** zůstává prázdná.

Kontrola aplikací

- Při práci v systému Microsoft Windows 10 v režimu seznamu blokovaných aplikací mohou být pravidla blokování nesprávně použita, což může způsobit blokování aplikací, které nejsou v pravidlech specifikovány.
- Když jsou progresivní webové aplikace (PWA) blokovány součástí Kontrola aplikací, appManifest.xml je v sestavě označen jako blokovaná aplikace.

Kontrola zařízení

- Přístup k tiskovým zařízením, která byla přidána do seznamu důvěryhodných, je blokován pravidly blokování zařízení a sběrnice.
- U zařízení MTP je podporováno ovládání operací čtení, zápisu a připojení, pokud používáte integrované ovladače Microsoft operačního systému. Pokud uživatel nainstaluje vlastní ovladač pro práci se zařízením (například jako součást iTunes nebo Android Debug Bridge), ovládání operací čtení a zápisu nemusí fungovat.
- Při práci se zařízeními MTP se přístupová pravidla po opětovném připojení zařízení změní.
- Pokud přidáváte zařízení do seznamu důvěryhodných na základě masky modelu a používáte znaky, které jsou zahrnuty v ID, ale ne v názvu modelu, tato zařízení se nepřidají. Na pracovní stanici budou tato zařízení přidána do seznamu důvěryhodných na základě masky ID.

Kontrola webu

- Formáty OGV a WEBM nejsou podporovány.
- Protokol RTMP není podporován.

Adaptivní kontrola anomálií

- Doporučuje se automaticky vytvářet výjimky na základě události. Při ručním přidání výjimky přidejte při zadávání cílového objektu na začátek cesty znak `*`.
- Sestavu pravidel adaptivního řízení anomálií nelze vygenerovat, pokud ukázka obsahuje byť jen jednu událost, jejíž název obsahuje více než 260 znaků.
- Přidávání výjimek z úložiště aktivace pravidel součásti Adaptivní kontrola anomálií není podporováno, pokud vlastnosti objektu nebo procesu mají hodnotu skládající se z více než 256 znaků (například cesta k cílovému objektu). Výjimku můžete přidat ručně v nastavení zásad. Výjimku také můžete přidat do zprávy o aktivovaných pravidlech součásti Adaptivní kontrola anomálií.

Drive Encryption (FDE)

- Aby šifrování pevného disku fungovalo správně, po instalaci aplikace musíte restartovat operační systém.
- Ověřovací agent nepodporuje hieroglyfy ani speciální znaky `|` a `\`.
- Pro optimální výkon počítače po šifrování je nutné, aby procesor podporoval sadu instrukcí AES-NI (Intel Advanced Encryption Standard New Instructions). Pokud procesor AES-NI nepodporuje, výkon počítače se může snížit.
- Pokud existují procesy, které se pokoušejí získat přístup k šifrovaným zařízením před tím, než aplikace k těmto zařízením udělí přístup, aplikace zobrazí varování, že takové procesy musí být ukončeny. Jestliže procesy nelze ukončit, znovu připojte šifrovaná zařízení.
- Jedinečné ID pevných disků se zobrazují ve statistikách šifrování zařízení v obráceném formátu.
- Nedoporučuje se formátovat zařízení, zatímco jsou šifrována.
- Pokud je k počítači současně připojeno více vyměnitelných jednotek, lze zásady šifrování použít pouze na jednu vyměnitelnou jednotku. Po opětovném připojení vyměnitelných zařízení se zásady šifrování použijí správně.
- Na silně fragmentovaném pevném disku může dojít k selhání šifrování. Defragmentujte pevný disk.
- Pokud jsou pevné disky šifrovány, hibernace je blokována od okamžiku, kdy se spustí úloha šifrování, do prvního restartování počítače se systémem Microsoft Windows 7/8/8.1/10 a po instalaci šifrování pevného disku do prvního restartování operačního systému Microsoft Windows 8/8.1/10. Při dešifrování pevných disků je hibernace blokována od okamžiku úplného dešifrování spouštěcí jednotky až do prvního restartování operačního systému. Když je v systému Microsoft Windows 8/8.1/10 povolena možnost **Rychlý start**, blokování hibernace vám zabrání ve vypnutí operačního systému.
- Počítače se systémem Windows 7 neumožňují během obnovení měnit heslo, když je disk šifrován technologií BitLocker. Po zadání klíče obnovení a načtení operačního systému aplikace Kaspersky Endpoint Security nebude vyzývat uživatele ke změně hesla nebo kódu PIN. Není tedy možné nastavit nové heslo ani kód PIN. Tento problém vychází ze zvláštností tohoto operačního systému. Chcete-li pokračovat, musíte znovu zašifrovat pevný disk.
- Nedoporučuje se používat nástroj xbootmgr.exe, když jsou povoleni další poskytovatelé, například Dispečer, Síť nebo Ovladače.
- V počítači, na kterém je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows, není formátování šifrované vyměnitelné jednotky podporováno.
- Formátování šifrované vyměnitelné jednotky pomocí systému souborů FAT32 není podporováno (jednotka je zobrazena jako šifrovaná). Chcete-li jednotku naformátovat, přeformátujte ji pomocí systému souborů NTFS.
- Podrobnosti o obnovení operačního systému ze záložní kopie na šifrované zařízení GPT najdete ve znalostní bázi technické podpory.
- Na jednom šifrovaném počítači nemůže koexistovat více agentů stahování.
- Je nemožné získat přístup k vyměnitelné jednotce, která byla dříve zašifrována na jiném počítači, pokud jsou splněny všechny následující podmínky současně:
  - Neexistuje připojení k serveru Kaspersky Security Center.
  - Uživatel se pokouší o autorizaci pomocí nového tokenu nebo hesla.

Pokud nastane podobná situace, restartujte počítač. Po restartování počítače bude udělen přístup k šifrované vyměnitelné jednotce.

- Zjišťování zařízení USB pomocí ověřovacího agenta nemusí být podporováno, pokud je v nastavení systému BIOS povolen režim xHCI pro USB.
- Kaspersky Disk Encryption (FDE) pro část SSD zařízení, která se používá pro ukládání nejčastěji používaných dat do mezipaměti, není pro zařízení SSHD podporována.
- Šifrování pevných disků ve 32bitových operačních systémech Microsoft Windows 8/8.1/10 spuštěném v režimu UEFI není podporováno.
- Před opětovným zašifrováním dešifrovaného pevného disku restartujte počítač.
- Šifrování pevného disku není kompatibilní s aplikací Kaspersky Anti-Virus pro UEFI. Nedoporučuje se používat šifrování pevného disku v počítačích, na kterých je nainstalována aplikace Kaspersky Anti-Virus pro UEFI.
- Vytváření účtů agenta ověřování na základě účtů Microsoft je podporováno s následujícími omezeními:
  - Technologie jednotného přihlášení (SSO) není podporována.
  - Automatické vytváření účtů agenta ověřování není podporováno, pokud je vybrána možnost vytváření účtů pro uživatele, kteří se do systému přihlásí v posledních N dnech.
- Pokud má název účtu ověřovacího agenta formát <doména> / <název účtu Windows>, po změně názvu počítače musíte také změnit názvy účtů, které byly vytvořeny pro místní uživatele tohoto počítače. Představte si například, že v počítači `Ivan` je místní uživatel `Ivan` a pro tohoto uživatele byl vytvořen účet ověřovacího agenta s názvem `Ivan/Ivan`. Pokud byl název počítače `Ivan` změněn na `Ivan-PC`, musíte změnit název účtu Ověřovacího agenta pro uživatele `Ivan` z `Ivan/Ivan` na `Ivan-PC/Ivan`. Název účtu můžete spravovat pomocí místní úlohy správy Ověřovacího agenta. Před změnou názvu účtu je možné ověřování v prostředí před spuštěním pomocí starého názvu (například `Ivan/Ivan`).
- Pokud má uživatel povolen přístup k počítači zašifrovanému pomocí technologie Kaspersky Disk Encryption pouze pomocí tokenu a tento uživatel musí dokončit postup obnovení přístupu, ujistěte se, že tomuto uživateli je po přístupu k šifrovanému počítači udělen přístup založený na hesle. Heslo, které uživatel nastavil při obnovení přístupu, nemusí být uloženo. V takovém případě bude uživatel muset při příštím restartování počítače znovu dokončit postup pro obnovení přístupu k zašifrovanému počítači.
- Při dešifrování pevného disku pomocí nástroje pro obnovení FDE může proces dešifrování skončit chybou, pokud jsou data na zdrojovém zařízení přepsána dešifrovanými daty. Část dat na pevném disku zůstane šifrovaná. Při použití nástroje pro obnovení FDE se doporučuje zvolit možnost uložení dešifrovaných dat do souboru v nastavení dešifrování zařízení.
- Pokud bylo heslo ověřovacího agenta změněno, zobrazí se zpráva obsahující text *Vaše heslo bylo úspěšně změněno. Klikněte na tlačítko OK* a uživatel restartuje počítač, nové heslo se neuloží. Pro následné ověření v prostředí před spuštěním je nutné použít staré heslo.
- Šifrování disku není kompatibilní s technologií Intel Rapid Start.
- Šifrování disku není kompatibilní s technologií ExpressCache.
- V některých případech při pokusu o dešifrování šifrované jednotky pomocí nástroje FDE Recovery Tool nástroj po dokončení procedury „Request-Response“ omylem detekuje stav zařízení jako „nezašifrovaný“. Protokol nástroje zobrazuje událost uvádějící, že zařízení bylo úspěšně dešifrováno. V takovém případě musíte restartovat postup obnovy dat a dešifrovat zařízení.

- Po aktualizaci pluginu Kaspersky Endpoint Security pro Windows ve webové konzole se ve vlastnostech klientského počítače nezobrazí klíč pro obnovení nástroje BitLocker, dokud nebude služba Webová konzola restartována.

- Další omezení podpory šifrování celého disku a seznam zařízení, pro která je šifrování pevných disků s omezeními podporováno, najdete ve znalostní bázi technické podpory.

Šifrování na úrovni souborů (FLE).

- V operačních systémech rodiny Microsoft Windows Embedded není šifrování souborů a složek podporováno.
- Po instalaci aplikace musíte restartovat operační systém, aby šifrování souborů a složek fungovalo správně.
- Pokud je šifrovaný soubor uložen v počítači, který má k dispozici funkce šifrování, a přistupujete k němu z počítače, kde šifrování není k dispozici, bude k tomuto souboru poskytnut přímý přístup. Šifrovaný soubor, který je uložen v síťové složce v počítači, který má k dispozici funkce šifrování, je zkopírován v dešifrované podobě do počítače, který nemá k dispozici funkce šifrování.
- Před šifrováním souborů pomocí aplikace Kaspersky Endpoint Security pro systém Windows se doporučuje dešifrovat soubory, které byly zašifrovány pomocí systému šifrování souborů.
- Po zašifrování souboru se jeho velikost zvětší o 4 kB.
- Po zašifrování souboru se ve vlastnostech souboru nastaví atribut *Archiv*.
- Pokud má rozbalený soubor ze šifrovaného archivu stejný název jako již existující soubor ve vašem počítači, tento soubor může být přepsán novým souborem, který je rozbalen ze šifrovaného archivu. Uživatel není o operaci přepsání informován.
- Rozhraní Mobilní správce souborů nezobrazuje zprávy o chybách, ke kterým dojde během jeho provozu.
- Aplikace Kaspersky Endpoint Security pro Windows nespustí Mobilní správce souborů v počítači, na kterém je nainstalována součást Šifrování na úrovni souborů.
- Rozhraní Mobilní správce souborů nelze použít k získání přístupu k vyměnitelné jednotce, pokud jsou zároveň splněny následující podmínky:
  - Neexistuje připojení k aplikaci Kaspersky Security Center.
  - V počítači je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows.
  - Na počítači nebylo provedeno šifrování dat (FDE nebo FLE).

  V tomto případě není přístup možný, ani když znáte heslo pro rozhraní Mobilní správce souborů.
- Při použití šifrování souboru je aplikace nekompatibilní s poštovním klientem Sylpheed.
- Aplikace Kaspersky Endpoint Security pro systém Windows nepodporuje pravidlo omezení přístupu k šifrovaným souborům pro některé aplikace. Důvodem je skutečnost, že některé operace se soubory provádí aplikace třetí strany. Například kopírování souborů provádí správce souborů, nikoli samotná aplikace. Jestliže je poštovnímu klientovi Outlook odepřen přístup k šifrovaným souborům, Kaspersky Endpoint Security mu umožní přístup k šifrovanému souboru, pokud uživatel zkopíroval soubory do e-mailové zprávy prostřednictvím schránky nebo pomocí funkce přetažení. Operaci kopírování provedl správce souborů, pro který nejsou stanovena pravidla omezení přístupu k zašifrovaným souborům, tj. přístup je povolen.
- Změna nastavení souboru stránky není podporována. Operační systém používá výchozí hodnoty namísto zadaných hodnot parametrů.
- Při práci se šifrovanými vyměnitelnými jednotkami používejte bezpečné odebrání. Nemůžeme zaručit integritu dat, pokud vyměnitelná jednotka není bezpečně odebrána.
- Po zašifrování souborů budou jejich nezašifrované originály bezpečně odstraněny.

- Synchronizace offline souborů pomocí mezipaměti na straně klienta (CSC) není podporována. Doporučuje se zakázat offline správu sdílených prostředků na úrovni zásad skupiny. Soubory, které jsou v režimu offline, lze upravovat. Po synchronizaci mohou být změny provedené v offline souboru ztraceny. Podrobnosti týkající se podpory mezipaměti na straně klienta (CSC) při použití šifrování naleznete ve znalostní bázi technické podpory.

- Vytvoření šifrovaného archivu v kořenovém adresáři pevného disku systému není podporováno.

- Při přístupu k šifrovaným souborům v síti se mohou vyskytnout problémy. Doporučuje se přesunout soubory do jiného zdroje nebo zajistit, aby počítač používaný jako souborový server byl spravován stejným serverem pro správu aplikace Kaspersky Security Center.

- Změna rozložení klávesnice může způsobit zablokování okna pro zadání hesla pro šifrovaný samorozbalovací archiv. Chcete-li tento problém vyřešit, zavřete okno pro zadání hesla, přepněte na rozložení klávesnice ve vašem operačním systému a znovu zadejte heslo pro šifrovaný archiv.

- Pokud se šifrování souborů používá v systémech, které mají na jednom disku více oddílů, doporučujeme použít možnost, která automaticky určuje velikost souboru pagefile.sys. Po restartování počítače se může soubor pagefile.sys přesouvat mezi diskovými oddíly.

- Po použití pravidel šifrování souborů, včetně souborů ve složce Dokumenty, se ujistěte, že uživatelé, na které bylo šifrování aplikováno, mohou úspěšně přistupovat k šifrovaným souborům. Chcete-li tak učinit, nechte každého uživatele přihlásit se do systému, když je k dispozici připojení k aplikaci Kaspersky Security Center. Pokud se uživatel pokusí získat přístup k šifrovaným souborům bez připojení k aplikaci Kaspersky Security Center, může systém přestat reagovat.

- Pokud jsou systémové soubory nějak zahrnuty do rozsahu šifrování na úrovni souborů, mohou se v sestavách objevit události týkající se chyb při šifrování těchto souborů. Soubory uvedené v těchto událostech nejsou ve skutečnosti šifrovány.

- Procesy PICO nejsou podporovány.

- Cesty rozlišující velká a malá písmena nejsou podporovány. Když se použijí pravidla šifrování nebo dešifrování, cesty v událostech produktu se zobrazí malými písmeny.

- Nedoporučuje se šifrovat soubory, které systém používá při spuštění. Pokud jsou tyto soubory zašifrovány, může pokus o přístup k zašifrovaným souborům bez připojení k aplikaci Kaspersky Security Center způsobit zablokování systému nebo vést k výzvám k přístupu k nezašifrovaným souborům.

- Pokud jsou vyměnitelné jednotky šifrovány s podporou přenosného režimu, nelze kontrolu věku hesla deaktivovat.

- Pokud uživatelé společně pracují se souborem v síti podle pravidel FLE prostřednictvím aplikací, které používají metodu mapování souboru do paměti (například WordPad nebo FAR) a aplikací určených pro práci s velkými soubory (například Notepad ++), soubor v nezašifrované formě může být blokován na dobu neurčitou bez možnosti přístupu k němu z počítače, na kterém se nachází.

- Šifrování souborů ve složkách synchronizace OneDrive není podporováno. Přidání složek s již zašifrovanými soubory do seznamu synchronizace OneDrive může mít za následek ztrátu dat v zašifrovaných souborech.

- Když je nainstalována součást Šifrování na úrovni souborů, v režimu WSL (Windows Subsystem for Linux) nefunguje správa uživatelů a skupin.

- Když je nainstalována součást Šifrování na úrovni souborů, pro přejmenování a mazání souborů není podporováno rozhraní POSIX (Portable Operating System Interface).

- Po aktualizaci aplikace Kaspersky Endpoint Security pro systém Windows verze 11.0.1 nebo starší platí, že chcete-li získat přístup k zašifrovaným souborům po restartování počítače, zkontrolujte, zda je spuštěn

Síťový agent. Síťový agent se spouští se zpožděním, takže k zašifrovaným souborům nemáte přístup ihned po načtení operačního systému. Není třeba čekat na spuštění Síťového agenta po dalším spuštění počítače.

Další omezení

- V operačních systémech serveru se nezobrazuje žádné varování týkající se nutnosti pokročilé dezinfekce.
- Webové adresy, které jsou přidány do seznamu důvěryhodných, mohou být nesprávně zpracovány.
- Kaspersky Endpoint Security sleduje provoz HTTP, který odpovídá standardům RFC 2616, RFC 7540, RFC 7541 a RFC 7301. Pokud aplikace Kaspersky Endpoint Security zjistí v provozu HTTP jiný formát pro výměnu dat, toto připojení zablokuje, aby zabránila stahování škodlivých souborů z internetu.
- Kaspersky Endpoint Security nepodporuje standard RFC9218 pro protokol HTTP/2. Pokud aplikace Kaspersky Endpoint Security zjistí v provozu tento formát pro výměnu dat, toto připojení zablokuje a v prohlížeči se zobrazí chyba ERR_HTTP2_PROTOCOL_ERROR. Pokud potřebujete přístup k tomuto webovému prostředku, můžete jej vyloučit z kontroly šifrovaných připojení nebo kontaktovat technickou podporu a požádat ji o bezpečnostní opravu.
- System Watcher. Nezobrazují se úplné informace o procesech.
- Při prvním spuštění aplikace Kaspersky Endpoint Security pro systém Windows může být digitálně podepsaná aplikace dočasně umístěna do nesprávné skupiny. Digitálně podepsaná aplikace bude později zařazena do správné skupiny.
- Při kontrole pošty s příponou součásti Ochrana před hrozbami v poště pro Microsoft Outlook se doporučuje použít režim Exchange s mezipamětí (možnost Použít režim Exchange s mezipamětí).
- Úloha *antivirové kontroly* nepodporuje 64bitovou verzi aplikace Microsoft Outlook. To znamená, že aplikace Kaspersky Endpoint Security nekontroluje soubory x64 aplikace Outlook (soubory PST a OST), i když je pošta součástí rozsahu kontroly.
- Při přechodu z používání globální služby Kaspersky Security Network na privátní službu Kaspersky Security Network nebo naopak je v aplikaci Kaspersky Security Center 10 v zásadách konkrétního produktu zakázána možnost účastnit se služby Kaspersky Security Network. Po přepnutí si pečlivě přečtěte text Prohlášení ke službě Kaspersky Security Network a potvrďte svůj souhlas s účastí v KSN. Text prohlášení si můžete přečíst v rozhraní aplikace nebo při úpravách zásad produktu.
- Během opětovné kontroly škodlivého objektu, který byl blokován softwarem jiného výrobce, není uživatel upozorněn, když je hrozba znovu zjištěna. Událost opětovné detekce ohrožení se zobrazí ve zprávě o produktu a ve zprávě Kaspersky Security Center 10.
- Součást Endpoint Sensor nelze nainstalovat v systému Microsoft Windows Server 2008.
- Zpráva Kaspersky Security Center 10 o šifrování zařízení nebude obsahovat informace o zařízeních, která byla šifrována nástrojem Microsoft BitLocker na platformách serveru nebo na pracovních stanicích, na kterých není nainstalována součást Kontrola zařízení.
- Když používáte hierarchii zásad, nastavení v části Šifrování vyměnitelných jednotek v podřízené zásadě jsou přístupná pro úpravy, pokud nadřazená zásada úpravy těchto nastavení nezakazuje.
- Chcete-li zajistit správné fungování výjimek pro ochranu sdílených složek před externím šifrováním, v nastavení operačního systému musíte povolit funkci auditování přihlášení.
- Pokud je povolena ochrana sdílených složek, Kaspersky Endpoint Security pro systém Windows sleduje pokusy o šifrování sdílených složek pro každou relaci vzdáleného přístupu, která byla spuštěna před spuštěním aplikace Kaspersky Endpoint Security pro systém Windows, včetně případů, kdy byl počítač, ze kterého byla relace vzdáleného přístupu spuštěna, přidán k výjimkám. Pokud nechcete, aby aplikace Kaspersky Endpoint Security pro systém Windows sledovala pokusy o šifrování sdílených složek pro relace vzdáleného přístupu, které byly spuštěny z počítače, který byl přidán k výjimkám, a které byly spuštěny před spuštěním aplikace Kaspersky Endpoint Security pro systém Windows, ukončete a znovu navažte relaci

vzdáleného přístupu nebo restartujte počítač, na kterém je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows.

- Pokud je úloha aktualizace spuštěna s oprávněními konkrétního uživatelského účtu, opravy produktu se při aktualizaci ze zdroje, který vyžaduje autorizaci, nestáhnou.
- Spuštění aplikace může selhat kvůli nedostatečnému výkonu systému. Chcete-li tento problém vyřešit, použijte možnost Ready Boot nebo zvyšte časový limit operačního systému pro spuštění služeb.
- Aplikace nemůže fungovat v nouzovém režimu.
- Abyste zajistili, že aplikace Kaspersky Endpoint Security po systém Windows verze 11.5.0 a 11.6.0 může správě pracovat se softwarem Cisco AnyConnect, musíte nainstalovat Compliance Module verze 4.3.183.2048 nebo novější. Další informace o kompatibilitě s nástrojem Cisco Identity Services Engine najdete v dokumentaci společnosti Cisco.
- Nemůžeme zaručit, že ovládání zvuku bude fungovat před prvním restartem po instalaci aplikace.
- Když jsou povoleny soubory trasování se střídáním, pro součást AMSI a plugin aplikace Outlook se nevytváří žádné trasování.
- Trasování výkonu nelze v systému Windows Server 2008 shromažďovat ručně.
- Trasování výkonu pro typ trasování „Restartovat“ není podporováno.
- Úloha kontroly dostupnosti KSN již není podporována.
- Vypnutí možnosti „Zakázat externí správu systémových služeb“ vám neumožní zastavit službu aplikace, která byla nainstalována s parametrem `AMPPL=1` (ve výchozím nastavení je počínaje operačním systémem Windows 10RS2 hodnota parametru nastavena na `1`). Parametr `AMPPL` s hodnotou `1` umožňuje použití technologie Protection Processes pro službu produktu.
- Chcete-li spustit vlastní kontrolu složky, musí mít uživatel, který vlastní kontrolu spouští, oprávnění ke čtení atributů této složky. V opačném případě nebude možné kontrolu vlastní složky provést a skončí chybou.
- Když pravidlo kontroly definované v zásadě obsahuje cestu bez znaku `\` na konci, například `C:\složka1\složka2`, bude spuštěna kontrola pro cestu C:\složka1\.
- Při upgradu aplikace z verze 11.1.0 na 11.6.0 se nastavení součásti Ochrana AMSI obnoví na výchozí hodnoty.
- Pokud používáte zásady omezení softwaru (SRP), počítač se nemusí načíst (černá obrazovka). Doporučujeme změnit nastavení SRP následujícím způsobem: nastavte u parametru **Použít zásady omezení softwaru u následujících objektů** hodnotu **Všechny soubory softwaru kromě knihoven (jako např. soubory DLL)** a u pravidel pro cesty k souborům aplikace (`C:\Program Files\Common Files\Kaspersky Lab` a `C:\Program Files\Kaspersky Lab`) přidejte úroveň zabezpečení **Neomezená**. Podrobnosti o používání SRP najdete v *dokumentaci společnosti Microsoft*.
- Správa nastavení pluginu aplikace Outlook prostřednictvím rozhraní Rest API není podporována.
- Nastavení spuštění úlohy pro konkrétního uživatele nelze přenášet mezi zařízeními pomocí konfiguračního souboru. Po použití nastavení z konfiguračního souboru ručně zadejte uživatelské jméno a heslo.
- Po instalaci aktualizace nebude úloha kontroly integrity fungovat, dokud nebude restartován systém, aby se aktualizace použila.
- Pokud se úroveň otočeného trasování změní pomocí nástroje pro vzdálenou diagnostiku, aplikace Kaspersky Endpoint Security pro systém Windows nesprávně zobrazí prázdnou hodnotu pro úroveň

trasování. Trasovací soubory se však zapisují podle správné úrovně trasování. Když se úroveň otočeného trasování změní prostřednictvím místního rozhraní aplikace, úroveň trasování se správně upraví, ale nástroj pro vzdálenou diagnostiku nesprávně zobrazí úroveň trasování, která byla naposledy definována obslužným programem. To může způsobit, že správce nebude mít aktuální informace o aktuální úrovni trasování, a pokud uživatel ručně změní úroveň trasování v místním rozhraní aplikace, nemusí ve trasování existovat relevantní informace.

- V místním rozhraní neumožňuje nastavení funkce Ochrana heslem změnit název účtu správce (ve výchozím nastavení KLAdmin). Chcete-li změnit název účtu správce, musíte funkci Ochrana heslem zakázat, poté ji povolit a zadat nový název účtu správce.

- Kaspersky Endpoint Security sleduje provoz HTTP, který odpovídá standardům RFC 2616, RFC 7540, RFC 7541 a RFC 7301. Pokud aplikace Kaspersky Endpoint Security zjistí v provozu HTTP jiný formát pro výměnu dat, toto připojení zablokuje, aby zabránila stahování škodlivých souborů z internetu.

- Při kontrole šifrovaného připojení aplikace Kaspersky Endpoint Security vynucuje HTTP/1.

- Aplikace Kaspersky Endpoint Security je v případě instalace na server Windows Server 2019 nekompatibilní s Dockerem. Nasazení kontejnerů Docker na počítač s aplikací Kaspersky Endpoint Security způsobí selhání (BSOD).

Slovníček pojmů

Aktivní klíč

Klíč, který je aplikací aktuálně používán.

Antivirové databáze

Databáze, které obsahují informace o hrozbách pro zabezpečení počítače, o nichž společnost Kaspersky v době vydání antivirové databáze ví. Podpisy v antivirové databázi umožňují odhalovat škodlivý kód v kontrolovaných objektech. Antivirové databáze vytvářejí odborníci společnosti Kaspersky. Tyto databáze se aktualizují každou hodinu.

Archiv

Jeden nebo několik souborů zabalených do jednoho komprimovaného souboru. K zabalení a rozbalení dat je vyžadována specializovaná aplikace zvaná archivační program.

Další klíč

Klíč opravňující k použití aplikace, který však není aktuálně používaný.

Databáze phishingových webů

Seznam webových adres, u kterých odborníci společnosti Kaspersky zjistili, že souvisejí s phishingem. Databáze je pravidelně aktualizována a je součástí distribučního balíčku aplikací společnosti Kaspersky.

Databáze škodlivých webových adres

Seznam webových adres, jejichž obsah lze považovat za nebezpečný. Seznam je vytvářen odborníky společnosti Kaspersky. Je pravidelně aktualizován a je součástí distribučního balíčku aplikací společnosti Kaspersky.

Dezinfekce

Způsob zpracování infikovaných objektů, jehož výsledkem je úplné nebo částečné obnovení dat. Ne všechny infikované objekty je možné dezinfikovat.

Falešný alarm

Falešný alarm vznikne, když aplikace Kaspersky označí neinfikovaný soubor za infikovaný, protože je podpis souboru podobný podpisu viru.

Infikovaný soubor

Soubor obsahující škodlivý kód (při kontrole souboru byl zjištěn kód známého malwaru). Aplikace Kaspersky nedoporučuje používat takovéto soubory, protože mohou infikovat váš počítač.

Infikovatelný soubor

Soubor, který kvůli jeho struktuře nebo formátu mohou zneužít narušitelé jako „schránku“ pro uložení a šíření škodlivého kódu. Obvykle se jedná o spustitelné soubory, například s příponami souboru .com, .exe a .dll. U těchto souborů je velmi vysoké riziko napadení škodlivým kódem.

Licenční certifikát

Dokument, který společnost Kaspersky přenáší na uživatele společně se souborem klíče nebo aktivačním kódem. Obsahuje informace o licenci udělené uživateli.

Maska

Reprezentace názvu a přípony souboru pomocí zástupných znaků.

Masky souborů mohou obsahovat jakékoli znaky povolené v názvech souborů, včetně zástupných znaků:

- Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.

- Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složce s názvem `Složka` a jejích podložkách. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska. Maska ** je k dispozici pouze pro vytváření výjimek z kontroly.

- Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.

Mobilní správce souborů

Jedná se o aplikaci, která poskytuje rozhraní pro práci s šifrovanými soubory na vyměnitelných jednotkách v případě, že v počítači není k dispozici funkce šifrování.

Network Agent

Součást aplikace Kaspersky Security Center, která umožňuje interakci mezi administračním serverem a aplikacemi Kaspersky instalovanými v konkrétních síťových uzlech (pracovních stanicích nebo serverech). Tato součást je běžná pro všechny aplikace společnosti Kaspersky spouštěné v systému Windows. Vyhrazené verze součásti Network Agent jsou určeny pro aplikace spouštěné v jiných operačních systémech.

Normalizovaná forma adresy webového prostředku

Normalizovaná forma adresy webového prostředku je textovou reprezentací adresy webového prostředku, která je získána procesem normalizace. Normalizace je proces, při kterém je textová reprezentace webového prostředku změněna v souladu s určitými pravidly (například vyloučení přihlášení uživatele, hesla a portu připojení z textové reprezentace adresy webového prostředku; navíc je adresa webového prostředku změněna z velkých písmen na malá).

V souvislosti s činností součástí ochrany je účelem normalizace adresy webového prostředku zabránit vícenásobnému kontrolování webových adres, které mohou mít odlišnou syntaxi, a přesto být fyzicky ekvivalentní.

Příklad:

Nenormalizovaná forma adresy: www.Priklad.cz\.

Normalizovaná forma adresy: www.priklad.cz.

Objekt OLE

Soubor přílohy nebo soubor integrovaný do jiného souboru. Aplikace společnosti Kaspersky umožňují antivirovou kontrolu objektů OLE. Pokud například vložíte tabulku aplikace Microsoft Office Excel® do dokumentu aplikace Microsoft Office Word, tabulka bude kontrolována jako objekt OLE.

Ověřovací agent

Rozhraní umožňující dokončení ověřování pro přístup k šifrovaným pevným diskům a načtení operačního systému po zašifrování spustitelného pevného disku.

Rozsah kontroly

Objekty, které aplikace Kaspersky Endpoint Security kontroluje při provádění úlohy kontroly.

Rozsah ochrany

Objekty, které jsou neustále kontrolovány součástí Základní ochrana před hrozbami, když je spuštěná. Rozsahy ochrany pomocí různých součástí mají různé vlastnosti.

Skupina správy

Sada zařízení, které sdílí společné funkce, a sada aplikací společnosti Kaspersky, které jsou v těchto počítačích nainstalované. Zařízení jsou seskupena, aby je bylo možné jednodušeji spravovat jako jednu jednotku. Skupina může obsahovat jiné skupiny. Pro každou nainstalovanou aplikaci ve skupině lze vytvořit zásady skupiny a úlohy skupiny.

Trusted Platform Module

Mikročip vyvinutý pro poskytování základních funkcí souvisejících se zabezpečením (například k ukládání šifrovacích klíčů). Čip TPM je obvykle instalovaný na základní desce počítače a komunikuje se všemi ostatními součástmi systému prostřednictvím hardwarového rozhraní.

Úloha

Funkce prováděné aplikací společnosti Kaspersky jako úlohy, například: ochrana souborů v reálném čase, úplná kontrola zařízení, aktualizace databáze.

Vystavitel certifikátu

Certifikační středisko, které certifikát vystavilo.

Přílohy

Tato část obsahuje informace, které doplňují hlavní text dokumentu.

Příloha 1. Nastavení aplikace

Ke konfiguraci aplikace Kaspersky Endpoint Security můžete použít zásady, úlohy nebo rozhraní aplikace. Podrobné informace o součástech aplikace jsou uvedeny v odpovídajících částech.

Ochrana před souborovými hrozbami

Součásti Ochrana před souborovými hrozbami umožňuje zabránit infikování souborového systému počítače. Ve výchozím nastavení je součást Ochrana před souborovými hrozbami trvale uložena v paměti RAM počítače. Tato součást prohledává soubory na všech jednotkách počítače i na připojených jednotkách. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Součást prohledává soubory, k nimž přistoupil uživatel nebo aplikace. Pokud je zjištěn škodlivý soubor, aplikace Kaspersky Endpoint Security blokuje aktivitu tohoto souboru. Aplikace poté škodlivý soubor dezinfikuje nebo odstraní v závislosti na nastavení součásti Ochrana před souborovými hrozbami.

Když se pokusíte o přístup k souboru, jehož obsah je uložen v cloudu OneDrive, aplikace Kaspersky Endpoint Security stáhne a zkontroluje obsah tohoto souboru.

Nastavení součásti Ochrana před souborovými hrozbami

Parametr	Popis
Úroveň zabezpečení *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Pro ochranu před souborovými hrozbami může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy v aplikaci, se nazývají *úrovně zabezpečení*. • **Vysoká**. Při výběru této úrovně zabezpečení souborů kontroluje součást Ochrana před souborovými hrozbami všechny otevírané, ukládané a spouštěné soubory tím nejpřísnějším způsobem. Součást Ochrana před souborovými hrozbami kontroluje všechny typy souborů na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače. Kontroluje rovněž archivy, balíčky instalační služby a vložené objekty OLE. • **Doporučená**. Tuto úroveň zabezpečení souborů doporučují specialisté společnosti Kaspersky. Součást Ochrana před souborovými hrozbami kontroluje pouze zadané formáty souborů, a to na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače a také vložené objekty OLE. Součást Ochrana před souborovými hrozbami nekontroluje archivy ani instalační balíčky. • **Nízká**. Nastavení této úrovně zabezpečení souborů zajišťuje maximální rychlost kontroly. Součást Ochrana před souborovými hrozbami kontroluje pouze soubory se zadanými příponami, a to na všech pevných discích, vyměnitelných jednotkách a síťových jednotkách počítače. Součást Ochrana před souborovými hrozbami nekontroluje složené soubory.
Typy	**Všechny soubory**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security

souborů *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	zkontroluje všechny soubory bez výjimky (všechny formáty a přípony). **Soubory kontrolované podle formátu**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami. **Soubory kontrolované podle přípony**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.
Rozsah ochrany	Obsahuje objekty, které jsou kontrolovány součástí Ochrana před souborovými hrozbami. Objekt kontroly může být pevný disk, vyměnitelná jednotka, síťová jednotka, složka, soubor nebo více souborů definovaných maskou. Ve výchozím nastavení kontroluje součást Ochrana před souborovými hrozbami soubory spuštěné na všech pevných discích, síťových jednotkách či vyměnitelných jednotkách. Rozsah ochrany těchto objektů nelze změnit ani odstranit. Z kontroly také můžete vyloučit určitý objekt (například vyměnitelné jednotky).
Strojové učení a analýza signatur *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Metoda strojového učení a analýzy signatur používá databáze aplikace Kaspersky Endpoint Security, které obsahují popisy známých hrozeb a způsoby jejich neutralizace. Ochrana využívající tuto metodu poskytuje minimální přijatelnou úroveň zabezpečení. Na základě doporučení odborníků společnosti Kaspersky je metoda strojového učení a analýzy signatur vždy povolena.
Heuristická analýza *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Akce při zjištění hrozby	**Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.

	Blokovat. Pokud je vybrána tato možnost, bude součást Ochrana před souborovými hrozbami všechny infikované soubory automaticky blokovat, aniž by se je pokusila dezinfikovat. Před pokusem o dezinfekci nebo odstranění infikovaného souboru vytvoří aplikace Kaspersky Endpoint Security záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.
Kontrolovat pouze nové a změněné soubory	Kontroluje pouze nové soubory a soubory, které byly od posledního skenování změněny. To pomáhá zkrátit dobu skenování. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.
Kontrolovat archivy	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
Kontrolovat distribuční balíčky	Toto políčko povolí nebo zakáže kontrolu distribučních balíčků třetích stran.
Kontrolovat soubory ve formátu aplikací Microsoft Office	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Nerozbalovat velké složené soubory	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security zkontroluje složené soubory všech velikostí. Aplikace Kaspersky Endpoint Security kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.
Rozbalit složené soubory na pozadí	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům, které jsou větší než zadaná hodnota, před kontrolou těchto souborů. V tomto případě aplikace Kaspersky Endpoint Security rozbalí a zkontroluje složené soubory na pozadí. Aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům, které jsou menší než tato hodnota, až po rozbalení a kontrole těchto souborů. Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security umožní přístup ke složeným souborům pouze po rozbalení a kontrole souborů jakékoli velikosti.
Režim kontroly	Kaspersky Endpoint Security kontroluje soubory, ke kterým přistupuje uživatel, operační systém nebo aplikace spuštěná pod uživatelským účtem. **Chytrý režim**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekt na základě analýzy akcí v tomto objektu provedených. Například při práci s dokumentem aplikace Microsoft Office provede aplikace Kaspersky Endpoint Security kontrolu souboru při jeho úvodním otevření a konečném zavření. Prozatímní operace, které přepisují soubor, jeho kontrolu nespouštějí.

(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)	**Při přístupu a změnách**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty při každém pokusu o jejich otevření nebo změnu. **Při přístupu**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich otevření. **Při spuštění**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich spuštění.
Technologie iSwift *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.
Technologie iChecker *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).
Pozastavit součást Ochrana před souborovými hrozbami *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato možnost dočasně a automaticky pozastaví činnost součásti Ochrana před souborovými hrozbami v určený čas nebo při práci s určenými aplikacemi.

Ochrana před webovými hrozbami

Součást Ochrana před webovými hrozbami zabraňuje stahování škodlivých souborů z internetu a blokuje škodlivé a phishingové weby. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Aplikace Kaspersky Endpoint Security kontroluje pouze provoz HTTP, HTTPS a FTP. Aplikace Kaspersky Endpoint Security kontroluje adresy URL a IP adresy. Můžete určit porty, které bude Kaspersky Endpoint Security sledovat, nebo vybrat všechny porty.

Pro sledování provozu HTTPS je třeba povolit kontroly šifrovaných připojení.

Když se uživatel pokusí otevřít škodlivý nebo phishingový web, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).

Zpráva o odepření přístupu na web

Nastavení součásti Ochrana před webovými hrozbami

Parametr	Popis
Úroveň zabezpečení *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Pro ochranu před webovými hrozbami může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy v aplikaci, se nazývají *úrovně zabezpečení*. • **Vysoká**. Úroveň zabezpečení, při které součást Ochrana před webovými hrozbami provádí maximální kontrolu webového provozu uskutečněného prostřednictvím protokolů HTTP a FTP směrem k počítači. Součást Ochrana před webovými hrozbami bude podrobně kontrolovat všechny objekty webového provozu pomocí všech databází aplikace a provádět nejpodrobnější možnou heuristickou analýzu. • **Doporučená**. Úroveň zabezpečení e-mailů, která poskytuje optimální rovnováhu mezi výkonem aplikace Kaspersky Endpoint Security a zabezpečením webového provozu. Součást Ochrana před webovými hrozbami bude provádět heuristickou analýzu na úrovni **Střední kontrola**. Tuto úroveň zabezpečení webového provozu doporučují specialisté společnosti Kaspersky. • **Nízká**. Nastavení této úrovně zabezpečení webového provozu zajišťuje nejrychlejší kontrolu webového provozu. Součást Ochrana před webovými hrozbami bude provádět heuristickou analýzu na úrovni **Lehká kontrola**.
Akce při zjištění hrozby	**Blokovat stahování**. Pokud je vybrána tato možnost a ve webovém provozu je zjištěn infikovaný objekt, součást Ochrana před webovými hrozbami zablokuje přístup k tomuto objektu a v prohlížeči zobrazí zprávu.

	Informovat. Pokud je vybrána tato možnost a ve webovém provozu je zjištěn infikovaný objekt, aplikace Kaspersky Endpoint Security umožní tento objekt stáhnout do počítače, ale přidá informace o infikovaném objektu do seznamu aktivních hrozeb.
Porovnat adresu URL s databází škodlivých adres URL *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Kontrola odkazů za účelem zjištění, zda jsou zahrnuty do databáze škodlivých webových adres, umožňuje sledovat weby, které byly na seznamu zakázaných webů. Databáze škodlivých webových adres je spravována společností Kaspersky, je zahrnuta v instalačním balíčku aplikace a aktualizována během aktualizací databáze aplikace Kaspersky Endpoint Security.
Použít heuristickou analýzu *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Když se u webového provozu kontroluje přítomnost virů a dalších aplikací, které představují hrozbu, provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Porovnat adresu URL s databází phishingových adres URL *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Databáze phishingových webových adres zahrnuje webové adresy aktuálně známých webových stránek, které se používají ke spuštění phishingových útoků. Společnost Kaspersky doplňuje tuto databázi phishingových odkazů o adresy získané od mezinárodní organizace známé jako Anti-Phishing Working Group. Databáze phishingových webových adres je zahrnuta v instalačním balíčku aplikace a doplňována aktualizacemi databáze aplikace Kaspersky Endpoint Security.
Nekontrolovat webový provoz z důvěryhodných webových adres	Pokud je toto políčko zaškrtnuto, nebude součást Ochrana před webovými hrozbami kontrolovat obsah webových stránek nebo webů, jejichž adresy jsou uvedeny v seznamu důvěryhodných webových adres. Konkrétní adresu i masku adresy webové stránky nebo webu lze přidat do seznamu důvěryhodných webových adres.

Ochrana před hrozbami v poště

Součást Ochrana před hrozbami v poště v přílohách kontroluje, zda příchozí a odchozí e-maily obsahují viry nebo jiné hrozby. Tato součást také kontroluje zprávy, zda neobsahují škodlivé a phishingové odkazy. Ve výchozím nastavení je součást Ochrana před hrozbami v poště trvale uložena v paměti RAM počítače a prohledává všechny zprávy přijaté nebo odeslané pomocí protokolů POP3, SMTP, IMAP nebo NNTP nebo poštovního klienta Microsoft Office Outlook (MAPI). Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Součást Ochrana před hrozbami v poště nekontroluje zprávy, pokud je poštovní klient otevřen v prohlížeči.

Jestliže je v příloze detekován škodlivý soubor, Kaspersky Endpoint Security přejmenuje předmět zprávy: `[Zpráva je infikována] <předmět zprávy>` nebo `[Infikovaný objekt odstraněn] <předmět zprávy>`.

Tato součást komunikuje s e-mailovými klienty nainstalovanými v počítači. U poštovního klienta aplikace Microsoft Office Outlook je k dispozici rozšíření s dalšími parametry. Rozšíření Ochrana před hrozbami v poště se vloží do e-mailového klienta Microsoft Office Outlook během instalace aplikace Kaspersky Endpoint Security.

Nastavení součásti Ochrana před hrozbami v poště

Parametr	Popis
Úroveň zabezpečení *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Pro ochranu před hrozbami v poště může aplikace Kaspersky Endpoint Security použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy v aplikaci, se nazývají *úrovně zabezpečení*. • **Vysoká**. Je-li vybrána tato úroveň zabezpečení e-mailů, součást Ochrana před hrozbami v poště kontroluje e-mailové zprávy nejdůkladněji. Součást Ochrana před hrozbami v poště kontroluje příchozí a odchozí e-mailové zprávy a provede podrobnou heuristickou analýzu. Úroveň zabezpečení pošty **Vysoká** se doporučuje pro vysoce riziková prostředí. Příkladem takového prostředí je připojení k bezplatné e-mailové službě z domácí sítě, která není hlídaná centralizovanou e-mailovou ochranou. • **Doporučená**. Úroveň zabezpečení e-mailů, která poskytuje optimální rovnováhu mezi výkonem aplikace Kaspersky Endpoint Security a zabezpečením e-mailů. Součást Ochrana před hrozbami v poště kontroluje příchozí a odchozí e-mailové zprávy a provede heuristickou analýzu střední úrovně. Tato úroveň zabezpečení e-mailového provozu je doporučena odborníky společnosti Kaspersky. • **Nízká**. Při výběru této úrovně zabezpečení e-mailů bude součást Ochrana před hrozbami v poště kontrolovat pouze příchozí e-mailové zprávy a provádět zběžnou heuristickou analýzu. Nebude kontrolovat archivy, které jsou připojeny k e-mailovým zprávám. Na této úrovni zabezpečení e-mailů kontroluje součást Ochrana před hrozbami v poště e-mailové zprávy maximální rychlostí a využívá minimum prostředků operačního systému. **Nízká** úroveň zabezpečení e-mailů je doporučena pro dobře chráněná prostředí. Příkladem takovéhoto prostředí může být podniková síť LAN s centralizovaným zabezpečením pošty.
Akce při zjištění hrozby	**Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, Kaspersky Endpoint Security tento objekt odstraní. Aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci: `[Byl odstraněn infikovaný objekt] <předmět zprávy>`.

	Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace Kaspersky Endpoint Security k předmětu zprávy upozornění: `[Infikovaná zpráva]` <předmět zprávy>. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace Kaspersky Endpoint Security tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace Kaspersky Endpoint Security zablokuje přenos zprávy a poštovní klient zobrazí chybu. **Blokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace Kaspersky Endpoint Security k předmětu zprávy upozornění: `[Infikovaná zpráva] <předmět zprávy>`. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace Kaspersky Endpoint Security zablokuje přenos zprávy a poštovní klient zobrazí chybu.
Rozsah ochrany *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	*Rozsah ochrany* zahrnuje objekty, které součást při spuštění kontroluje: **Příchozí a odchozí zprávy** nebo **Pouze příchozí zprávy**. Chcete-li chránit své počítače, musíte kontrolovat pouze příchozí zprávy. Abyste zabránili odesílání infikovaných souborů v archivech, můžete zapnout kontrolu odchozích zpráv. Kontrolu odchozích zpráv můžete také zapnout, pokud chcete zabránit odesílání souborů v určitých formátech, například zvukových a obrazových souborů.
Kontrolovat přenosy POP3/SMTP/NNTP/IMAP	Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat součásti Ochrana před hrozbami v poště kontrolovat data přenášená prostřednictvím protokolů POP3, SMTP, NNTP a IMAP.
Připojovat rozšíření pro Microsoft Outlook	Pokud je políčko zaškrtnuto, kontrola e-mailových zpráv přenášených přes protokoly POP3, SMTP, NNTP a IMAP je povolena na straně rozšíření integrovaného do aplikace Microsoft Outlook. Pokud je e-mail kontrolován pomocí rozšíření pro aplikaci Microsoft Outlook, doporučujeme použít režim serveru Exchange s mezipamětí. Podrobnější informace o režimu serveru Exchange s mezipamětí a o doporučeních k jeho použití najdete ve znalostní bázi Microsoft Knowledge Base.
Heuristická analýza *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Kontrolovat připojené archivy	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE. Pokud aplikace Kaspersky Endpoint Security během kontroly zjistí v textu zprávy heslo k archivu, bude toto heslo použito ke kontrole obsahu archivu na škodlivé aplikace. V tomto případě se heslo neukládá. Archiv je během kontroly rozbalen. Pokud během rozbalování dojde k chybě aplikace, můžete ručně odstranit rozbalené soubory, které jsou uloženy na následující cestě: %systemroot%\temp. Soubory mají předponu PR.

Kontrola přiložených formátů sady Office	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Nekontrolovat archivy větší než N MB	Pokud je toto políčko zaškrtnuto, vyloučí součást Ochrana před hrozbami v poště z kontroly archivy připojené k e-mailovým zprávám, jejichž velikost překračuje zadanou hodnotu. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude součást Ochrana před hrozbami v poště kontrolovat archivy připojené k e-mailovým zprávám, a to bez ohledu na jejich velikost.
Nekontrolovat archivy déle než N s	Je-li políčko zaškrtnuto, doba přidělená kontrole archivů připojených k e-mailovým zprávám je omezena na zadanou dobu.
Filtr příloh	Funkce filtrování příloh se nepoužije na odchozí e-mailové zprávy. **Zakázat filtrování**. Pokud je tato možnost vybrána, nebude součást Ochrana před hrozbami v poště filtrovat soubory připojené k e-mailovým zprávám. **Přejmenovat přílohy vybraného typu**. Pokud je tato možnost vybrána, nahradí součást Ochrana před hrozbami v poště poslední znak v připojených souborech zadaných typů symbolem podtržítka (například priloha.doc_). Uživatel tedy musí soubor přejmenovat, aby jej mohl otevřít. **Odstranit přílohy vybraného typu**. Pokud je tato možnost vybrána, odstraní součást Ochrana před hrozbami v poště připojené soubory zadaných typů z e-mailových zpráv. V seznamu masek souborů můžete určit typy připojených souborů, které chcete přejmenovat v e-mailových zprávách nebo je z nich odstranit.

Ochrana před síťovými hrozbami

Součást Ochrana před síťovými hrozbami kontroluje příchozí síťový provoz a zjišťuje přítomnost aktivit typických pro síťové útoky. Pokud aplikace Kaspersky Endpoint Security zjistí pokus o útok na síť v počítači uživatele, zablokuje síťové připojení k útočícímu počítači.

Popisy aktuálně známých typů síťových útoků a způsoby, jak se jim bránit, jsou k dispozici v databázích aplikace Kaspersky Endpoint Security. Seznam síťových útoků, které je součást Ochrana před síťovými hrozbami schopna zjistit, se aktualizuje při aktualizacích databází a modulů aplikace.

Nastavení součásti Ochrana před síťovými hrozbami

Parametr	Popis
Detekujte útoky typu skenování portů a přehlcení sítě	*Přehlcení sítě* je útok na síťové zdroje organizace (například webové servery). Tento útok spočívá v odeslání velkého počtu požadavků za účelem přetížení šířky pásma síťových prostředků. Když k tomu dojde, uživatelé nebudou mít přístup k síťovým prostředkům organizace. Útoky typu *skenování portů* zahrnují skenování portů UDP, TCP a síťových služeb v počítači. Tento útok umožňuje útočníkovi určit stupeň zranitelnosti počítače před provedením nebezpečnějších typů síťových útoků. Skenování portů také umožňuje útočníkovi identifikovat operační systém v počítači a vybrat vhodné síťové útoky pro tento operační systém.

	Pokud je zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security sleduje síťový provoz, aby tyto útoky zjistila. Když je detekován útok, aplikace filtruje a blokuje provoz spojený s útokem. Pokud je tak proti počítači zahájen útok typu přehlcení sítě, aplikace sníží zatížení napadeného prostředku. Pokud je proti počítači zahájen útok typu skenování portů, zabrání aplikace Kaspersky Endpoint Security úniku dat v počítači. Detekci těchto typů útoků můžete zakázat v případě, že některé z vašich povolených aplikací provádějí operace, které jsou pro tyto typy útoků typické. To pomůže vyhnout se falešným poplachům.
Přidat útočící počítač do seznamu blokovaných počítačů na dobu N minut	Pokud je toto políčko zaškrtnuto, přidá součást Ochrana před síťovými hrozbami útočící počítač do seznamu blokovaných počítačů. Znamená to, že součást Ochrana před síťovými hrozbami bude síťové propojení s útočícím počítačem blokovat po zadanou dobu od prvního pokusu o síťový útok. Takové blokování automaticky chrání počítač uživatele před možnými budoucími síťovými útoky ze stejné adresy. Seznam bloků můžete zobrazit v okně nástroje Sledování sítě. Aplikace Kaspersky Endpoint Security vymaže seznam bloků při svém restartu a při změně nastavení součásti Ochrana před síťovými hrozbami.
Výjimky	Tento seznam obsahuje IP adresy, ze kterých součást Ochrana před síťovými hrozbami neblokuje síťové útoky. Aplikace Kaspersky Endpoint Security nezaznamená do protokolu informace o síťových útocích z IP adres, které jsou v seznamu výjimek.
Ochrana proti falšování adres MAC	Součástí útoku *falšování adres MAC* je změna adresy MAC síťového zařízení (síťové karty). V důsledku toho může útočník přesměrovat data odeslaná do zařízení na jiné zařízení a získat přístup k těmto datům. Aplikace Kaspersky Endpoint Security umožňuje blokovat útoky falšování adres MAC a zobrazovat oznámení o útocích.

Brána firewall

Brána firewall blokuje neoprávněné připojení k počítači při práci na internetu nebo v místní síti. Brána firewall také řídí síťovou aktivitu aplikací v počítači. To vám umožní chránit vaši firemní LAN před krádeží identity a jinými útoky. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a předdefinovaných *pravidel sítě*.

Pro interakci s aplikací Kaspersky Security Center se používá síťový agent. Brána firewall automaticky vytváří pravidla sítě požadovaná pro fungování aplikace a síťového agenta. Díky tomu brána firewall otevírá několik portů v počítači. Které porty jsou otevřeny, závisí na roli počítače (například distribuční bod). Další informace o portech, které se budou v počítači otevírat, naleznete v *nápovědě k aplikaci Kaspersky Security Center*.

Pravidla sítě

Pravidla sítě můžete konfigurovat na následujících úrovních:

- *Pravidla síťových paketů*. Pravidla síťových paketů vytvářejí omezení pro síťové pakety bez ohledu na aplikaci. Takováto pravidla omezují příchozí a odchozí provoz konkrétních portů vybraného datového protokolu. Aplikace Kaspersky Endpoint Security má předdefinovaná pravidla pro síťové pakety s oprávněními doporučenými odborníky společnosti Kaspersky.

- *pravidla sítě aplikace*. pravidla sítě aplikace vytvářejí omezení síťové aktivity konkrétní aplikace. Berou do úvahy nejen charakteristiky síťového paketu, ale také konkrétní aplikaci, které je síťový paket určen nebo která síťový paket vyslala.

Řízený přístup aplikací ke zdrojům, procesům a osobním údajům operačního systému umožňuje součást Prevence narušení hostitele pomocí *oprávnění aplikací*.

Při prvním spuštění aplikace provede brána firewall následující akce:

1. Zkontroluje zabezpečení aplikace pomocí stažených antivirových databází.
2. Zkontroluje zabezpečení webu ve službě Kaspersky Security Network.

   Doporučujeme vám zapojit se do služby Kaspersky Security Network, aby mohla tato služba fungovat ještě efektivněji.
3. Umístí aplikaci do jedné ze *skupin důvěryhodnosti*: Důvěryhodné, Nízké omezení, Vysoké omezení, Nedůvěryhodné.

   Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace. Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat.

   Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti pro součásti Brána firewall a Prevence narušení hostitele. Skupinu důvěryhodnosti nelze změnit pouze u součástí Brána firewall a Prevence narušení hostitele.

   Pokud jste účast v KSN odmítli nebo neexistuje žádná síť, aplikace Kaspersky Endpoint Security umístí aplikaci do skupiny důvěryhodnosti v závislosti na nastavení součásti Prevence narušení hostitele. Po obdržení reputace aplikace z KSN lze skupinu důvěryhodnosti změnit automaticky.
4. Blokuje síťovou aktivitu aplikace v závislosti na skupině důvěryhodnosti. Například aplikace ve skupině důvěrnosti s vysokým omezením nemohou používat žádná síťová připojení.

Při příštím spuštění aplikace ověří součást aplikace Kaspersky Endpoint Security integritu aplikace. Pokud je aplikace nezměněná, součást pro ni použije aktuální pravidla sítě. Pokud došlo ke změně aplikace, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spouštěna poprvé.

Priority pravidel sítě

Každé pravidlo má prioritu. Čím výše se pravidlo na seznamu nachází, tím vyšší je jeho priorita. Pokud je síťová aktivita přidána do několika pravidel, brána firewall ji reguluje podle pravidla s nejvyšší prioritou.

Pravidla síťových paketů mají vyšší prioritu než pravidla sítě pro aplikace. Pokud jsou pro stejný typ síťové aktivity určena pravidla síťových paketů i pravidla sítě pro aplikace, síťová aktivita bude zpracována podle pravidel síťových paketů.

pravidla sítě pro aplikace fungují následovně: pravidlo sítě pro aplikace zahrnuje pravidla přístupu založená na stavu sítě: *veřejná*, *místní* nebo *důvěryhodná*. Například aplikace ve skupině důvěryhodnosti s vysokým omezením nepovolují ve výchozím nastavení žádnou síťovou aktivitu v sítích všech stavů. Pokud je pro jednotlivé aplikace (nadřazenou aplikaci) zadáno pravidlo sítě, potom se podřízené procesy jiných aplikací spustí podle pravidla sítě nadřazené aplikace. Jestliže pro aplikaci neexistuje žádné pravidlo sítě, budou podřízené procesy spuštěny podle pravidla síťového přístupu skupiny důvěryhodnosti aplikace.

Například jste zakázali jakoukoli síťovou aktivitu v sítích všech stavů pro všechny aplikace s výjimkou prohlížeče X. Pokud spustíte instalaci prohlížeče Y (podřízený proces) z prohlížeče X (nadřazená aplikace), bude mít instalační program prohlížeče Y přístup k síti a stáhne si potřebné soubory. Po instalaci budou prohlížeči Y zamítnuta všechna síťová připojení podle nastavení brány firewall. Chcete-li zakázat síťovou aktivitu instalačního programu prohlížeče Y jako podřízený proces, musíte přidat pravidlo sítě pro instalační program tohoto prohlížeče.

Stavy síťového připojení

Brána firewall umožňuje řídit síťovou aktivitu v závislosti na stavu síťového připojení. Aplikace Kaspersky Endpoint Security přijímá stav síťového připojení z operačního systému počítače. Stav síťového připojení v operačním systému nastavuje uživatel při nastavování připojení. Stav síťového připojení můžete změnit v nastavení aplikace Kaspersky Endpoint Security. Brána firewall bude sledovat aktivitu sítě v závislosti na stavu sítě v nastavení aplikace Kaspersky Endpoint Security, a ne v operačním systému.

Síťové připojení může mít jeden z následujících typů stavu:

- **Veřejná síť**. Síť není chráněna antivirovými aplikacemi, bránami firewall ani filtry (například Wi-Fi v kavárně). Když uživatel používá počítač připojený k takovéto síti, brána firewall bude blokovat přístup k souborům a tiskárnám počítače. Externí uživatelé dále nebudou moci přistupovat k datům ve sdílených složkách a využívat vzdálený přístup k ploše počítače. Brána firewall filtruje síťovou aktivitu jednotlivých aplikací v závislosti na pravidlech sítě, které jsou pro ně nastaveny.

  Brána firewall ve výchozím nastavení přiřadí stav *Veřejná síť* například internetu. Stav v případě internetu nelze změnit.

- **Místní síť**. Síť pro uživatele s omezeným přístupem k souborům a tiskárnám v tomto počítači (například pro podnikovou síť LAN nebo domácí síť).

- **Důvěryhodná síť**. Bezpečná síť, ve které není počítač vystaven útokům nebo pokusům o neoprávněný přístup k datům. V rámci sítí s tímto stavem povolí brána firewall jakoukoli síťovou aktivitu.

Nastavení součásti Brána firewall

Parametr	Popis
Pravidla síťových paketů	Tabulka se seznamem pravidel síťových paketů. Pravidla síťových paketů slouží k uplatnění omezení na síťové pakety, bez ohledu na aplikaci. Takováto pravidla omezují příchozí a odchozí provoz konkrétních portů vybraného datového protokolu. Tabulka uvádí předem konfigurovaná pravidla síťových paketů, která doporučuje společnost Kaspersky pro optimální ochranu síťového provozu počítačů s operačním systémem Microsoft Windows. Brána firewall nastavuje prioritu uplatnění jednotlivých pravidel síťových paketů. Brána firewall zpracuje pravidla síťových paketů v pořadí, ve kterém jsou uvedeny v seznamu pravidel síťových paketů, shora dolů. Brána firewall vyhledá nejvyšší pravidlo síťových paketů, které je vhodné pro síťové připojení, a uplatní je tím, že povolí nebo zakáže síťovou aktivitu. Brána firewall pak ignoruje všechna následná pravidla síťových paketů pro konkrétní síťové připojení. Pravidla síťových paketů mají vyšší prioritu než pravidla sítě pro aplikace.
Síťová připojení	Tato tabulka obsahuje informace o síťových připojeních, které brána firewall detekuje v počítači. Ve výchozím nastavení je internetu přiřazen stav *Veřejná síť*. Stav v případě internetu nelze změnit.
Pravidla sítě	**Přílohy**

	Tabulka aplikací, které jsou ovládány součástí Brána firewall. Aplikace jsou přiřazovány do skupin důvěryhodnosti. Skupina důvěryhodnosti definuje práva, která aplikace Kaspersky Endpoint Security používá při řízení síťové aktivity aplikací. Můžete vybrat aplikaci z jednotného seznamu všech aplikací nainstalovaných v počítačích pod vlivem zásady a přidat aplikaci do skupiny důvěryhodnosti. **Pravidla sítě** Tabulka síťových pravidel pro aplikace, které jsou součástí skupiny důvěryhodnosti. V souladu s těmito pravidly brána firewall reguluje síťovou aktivitu aplikace nebo skupiny aplikací. Tabulka uvádí předdefinovaná pravidla sítě, která doporučují odborníci společnosti Kaspersky. Tato pravidla sítě byla přidána k optimální ochraně síťového provozu počítačů s operačními systémy Windows. Předdefinovaná pravidla sítě nelze odstranit.

Ochrana před útoky BadUSB

Některé viry mohou pozměnit firmware zařízení USB, aby ho operační systém omylem rozpoznal jako klávesnici. Virus tak může pod vaším uživatelským účtem provádět příkazy, které například stahují malware.

Součást Ochrana před útoky BadUSB brání tomu, aby se infikovaná zařízení USB napodobující klávesnici připojila k počítači.

Když je zařízení USB připojeno k počítači a identifikováno operačním systémem jako klávesnice, aplikace vyzve uživatele k zadání číselného kódu vygenerovaného aplikací pomocí této klávesnice nebo pomocí klávesnice na obrazovce (viz obrázek níže). Tento postup je známý jako autorizace klávesnice.

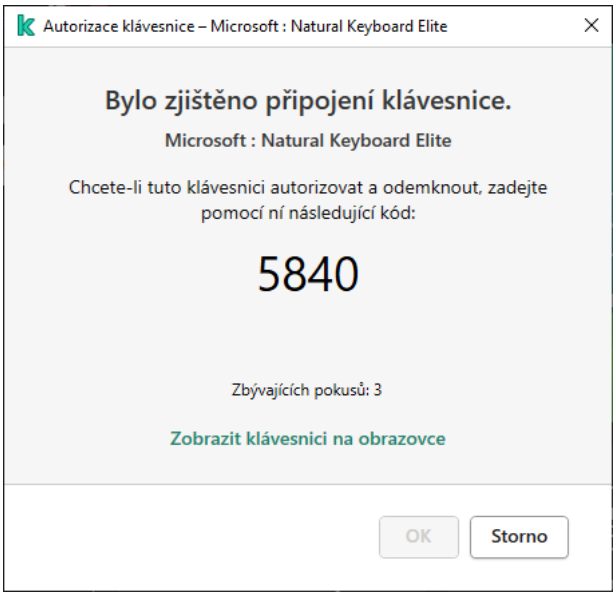
Pokud byl kód zadán správně, aplikace uloží parametry identifikace (kódy VID/PID klávesnice a číslo portu, ke kterému byla připojena) do seznamu autorizovaných klávesnic. Autorizaci není třeba opakovat po opětovném připojení klávesnice ani po restartování operačního systému.

Když autorizovanou klávesnici připojíte k jinému portu USB počítače, aplikace zobrazí výzvu k autorizaci této klávesnice znovu.

Pokud číselný kód zadáte nesprávně, aplikace vygeneruje nový kód. Na zadání číselného kódu máte tři pokusy. Pokud číselný kód zadáte nesprávně třikrát za sebou nebo okno **Autorizace klávesnice <Název klávesnice>** zavřete, aplikace vstup z této klávesnice zablokuje. Pokud klávesnici odpojíte a znovu připojíte nebo restartujete operační systém, aplikace vás k autorizaci klávesnice vyzve znovu.

Aplikace dovolí použití autorizované klávesnice a zablokuje klávesnici, která nebyla autorizována.

Součást Ochrana před útoky BadUSB není ve výchozím nastavení nainstalována. Pokud součást Ochrana před útoky BadUSB potřebujete, můžete ji přidat do vlastností instalačního balíčku před instalací aplikace nebo změnit dostupné komponenty aplikace po instalaci aplikace.



Autorizace klávesnice

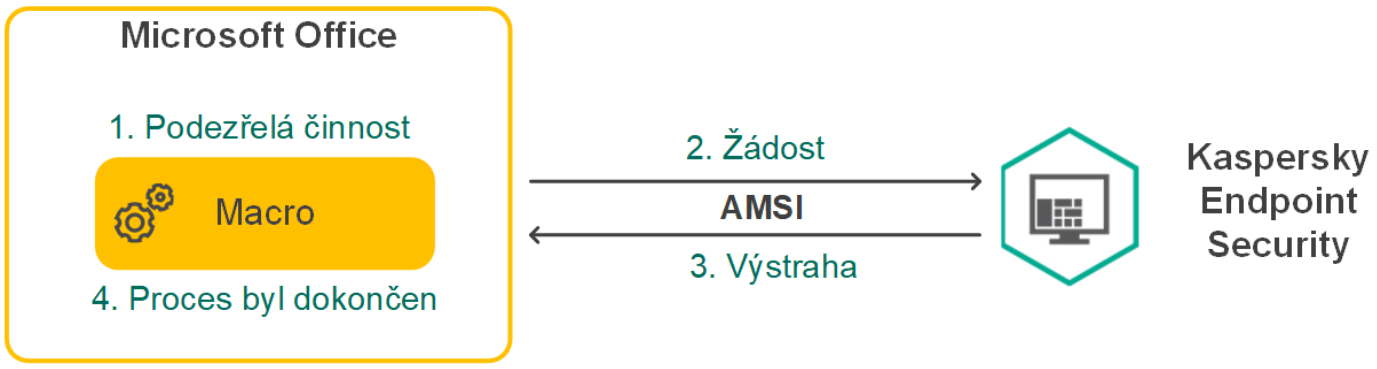
Nastavení součásti Ochrana před útoky BadUSB

Parametr	Popis
Zakázat klávesnici na obrazovce pro ověřování zařízení USB	Je-li políčko zaškrtnuto, aplikace blokuje použití klávesnice na obrazovce pro ověřování USB zařízení, ze kterého nelze ověřovací kód zadat.

Ochrana AMSI

Součást Ochrana AMSI je určen k podpoře rozhraní Antimalware Scan Interface od společnosti Microsoft. *Rozhraní AMSI (Antimalware Scan Interface)* umožňuje aplikacím třetích stran s podporou rozhraní AMSI odesílat objekty (například skripty prostředí PowerShell) do aplikace Kaspersky Endpoint Security za účelem další kontroly a přijímat výsledky kontroly těchto objektů. Aplikace třetích stran mohou zahrnovat například aplikace Microsoft Office (viz obrázek níže). Podrobnosti o rozhraní AMSI najdete v *dokumentaci společnosti Microsoft*.

Ochrana AMSI může pouze zjistit hrozby v aplikaci třetí strany a upozornit na ně, ale nemůže hrozby zpracovat. Aplikace třetí strany po obdržení oznámení týkající se hrozby nepovolí provedení škodlivých akcí (například se ukončí).



Příklad fungování AMSI

Ochrana AMSI může odmítnout žádost od aplikace třetí strany, a to například v případě, že tato aplikace překročí maximální počet žádostí v zadaném intervalu. Aplikace Kaspersky Endpoint Security odešle administračnímu serveru informace o odmítnuté žádosti od aplikace třetí strany. Součást Ochrana AMSI neodmítne žádosti od těchto aplikací třetích stran, u kterých je zaškrtnuto políčko **Neblokovat interakci se součástí Ochrana AMSI**.

Ochrana AMSI je k dispozici pro následující operační systémy pro pracovní stanice a servery:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Nastavení součásti Poskytovatel ochrany AMSI

Parametr	Popis
Kontrolovat archivy	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
Kontrolovat distribuční balíčky	Toto políčko povolí nebo zakáže kontrolu distribučních balíčků třetích stran.
Kontrolovat soubory ve formátu aplikací Microsoft Office	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Nerozbalovat velké složené soubory	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security zkontroluje složené soubory všech velikostí. Aplikace Kaspersky Endpoint Security kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.

Prevence zneužití

Součást Prevence zneužití detekuje programový kód, který využívá chyb zabezpečení v počítači k zneužití oprávnění správce nebo k provádění škodlivých činností. Zneužití může například využít útok v podobě přetečení vyrovnávací paměti. Za tímto účelem útočník odešle do zranitelné aplikace velké množství dat. Při zpracování těchto dat zranitelná aplikace spustí škodlivý kód. V důsledku tohoto útoku může útočník spustit neoprávněnou instalaci malwaru.

Pokud dojde k pokusu o spuštění spustitelného souboru ze zranitelné aplikace, které neprovedl uživatel, aplikace Kaspersky Endpoint Security spuštění tohoto souboru zablokuje nebo informuje uživatele.

Nastavení součásti Prevence zneužití

Parametr	Popis
Při zjištění zneužití	• **Blokovat akci**. Pokud je vybrána tato možnost, bude aplikace Kaspersky Endpoint Security při zjištění zneužití blokovat všechny akce, které jsou při pokusu o zneužití prováděny.

	• **Informovat**. Pokud je vybrána tato možnost a je zjištěno zneužití, aplikace Kaspersky Endpoint Security akce zneužití neblokuje, ale přidá informace o tomto zneužití do seznamu aktivních hrozeb.
Povolit ochranu paměti systémových procesů	Pokud je toto přepínací tlačítko v zapnuté poloze, aplikace Kaspersky Endpoint Security blokuje externí procesy, které se pokoušejí získat přístup k paměti systémových procesů.

Detekce chování

Součást Detekce chování přijímá data o akcích aplikací v počítači a tyto informace poskytuje jiným součástem ochrany, což zvyšuje jejich výkon.

Součást Detekce chování využívá podpisy BSS (Behavior Stream Signatures) pro aplikace. Pokud se činnost aplikace shoduje s podpisem BSS, aplikace Kaspersky Endpoint Security provede vybranou reaktivní akci. Fungování aplikace Kaspersky Endpoint Security na základě podpisů BSS poskytuje aktivní ochranu počítače.

Nastavení součásti Detekce chování

Parametr	Popis
Při detekci nebezpečné aktivity	• **Odstranit soubor**. V případě, že je vybrána tato možnost, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity odstraní spustitelný soubor škodlivého programu a vytvoří ve složce záloh jeho záložní kopii. • **Ukončit aplikaci**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity ukončí tuto aplikaci. • **Informovat**. Pokud je vybrána tato možnost a je zjištěna škodlivá aktivita aplikace, aplikace Kaspersky Endpoint Security tuto aplikaci neblokuje, ale přidá informace o škodlivé aktivitě aplikace do seznamu aktivních hrozeb.
Povolit ochranu sdílených složek proti externímu šifrování	Pokud je přepínací tlačítko v zapnuté poloze, aplikace Kaspersky Endpoint Security analyzuje aktivitu ve sdílených složkách. Pokud se tato aktivita shoduje se signaturou chování datového proudu, které je typické pro externí šifrování, aplikace Kaspersky Endpoint Security provede vybranou akci. Aplikace Kaspersky Endpoint Security zabraňuje externímu šifrování pouze u souborů uložených na médiích se souborovým systémem NTFS, která nejsou šifrována systémem EFS. • **Informovat**. Pokud je vybrána tato možnost, při zjištění pokusu o změnu souborů ve sdílených složkách přidá aplikace Kaspersky Endpoint Security informace o tomto pokusu o změnu souborů ve sdílených složkách do seznamu aktivních hrozeb. • **Blokovat připojení**. Pokud je vybrána tato možnost, při zjištění pokusu o změnu souborů ve sdílených složkách blokuje aplikace Kaspersky Endpoint Security síťovou aktivitu pocházející z počítače, který se pokouší změnit soubory, a vytvoří záložní kopie změněných souborů.

	Pokud je povolena součást Modul pro nápravu a je zaškrtnuta možnost **Blokovat připojení**, aplikace Kaspersky Endpoint Security obnoví změněné soubory ze záložních kopií.
Blokovat připojení po dobu N minut	Doba, po kterou bude aplikace Kaspersky Endpoint Security blokovat síťovou aktivitu vzdáleného počítače provádějícího šifrování sdílených složek.
Výjimky	Jedná se o seznam počítačů, jejichž pokusy o šifrování sdílených složek nebudou sledovány. Chcete-li použít seznam vyloučení počítačů z ochrany sdílených složek před externím šifrováním, musíte v zásadách auditu zabezpečení systému Windows povolit auditování přihlášení. Auditování je ve výchozím nastavení zakázáno. Podrobnější informace zásadách auditování přihlášení ve funkci Windows najdete na *webu společnosti Microsoft*.

Prevence narušení hostitele

Součást Prevence narušení hostitele zabraňuje aplikacím provádět akce, které mohou být pro operační systém nebezpečné, a kontroluje přístup k prostředkům operačního systému a osobním datům. Tato součást poskytuje ochranu počítače pomocí antivirových databází a cloudové služby Kaspersky Security Network.

Součást řídí provoz aplikací pomocí *oprávnění aplikací*. Oprávnění aplikací zahrnují následující parametry přístupu:

- Přístup k prostředkům operačního systému (například možnosti automatického spuštění, klíče registru)
- Přístup k osobním datům (jako jsou soubory a aplikace)

Síťová aktivita aplikací je ovládána bránou firewall pomocí *pravidel sítě*.

Během prvního spuštění aplikace provádí součást Prevence narušení hostitele následující akce:

1. Zkontroluje zabezpečení aplikace pomocí stažených antivirových databází.
2. Zkontroluje zabezpečení webu ve službě Kaspersky Security Network.

   Doporučujeme vám zapojit se do služby Kaspersky Security Network, čímž nám pomůžete zajistit účinnější fungování součásti Prevence narušení hostitele.

3. Umístí aplikaci do jedné ze *skupin důvěryhodnosti*: Důvěryhodné, Nízké omezení, Vysoké omezení, Nedůvěryhodné.

   Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace. Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat.

Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti pro součásti Brána firewall a Prevence narušení hostitele. Skupinu důvěryhodnosti nelze změnit pouze u součástí Brána firewall a Prevence narušení hostitele.

Pokud jste účast v KSN odmítli nebo neexistuje žádná síť, aplikace Kaspersky Endpoint Security umístí aplikaci do skupiny důvěryhodnosti v závislosti na nastavení součásti Prevence narušení hostitele. Po obdržení reputace aplikace z KSN lze skupinu důvěryhodnosti změnit automaticky.

4. Blokuje akce aplikace v závislosti na skupině důvěryhodnosti. Například aplikacím ze skupiny důvěryhodných s omezeným přístupem je odepřen přístup k modulům operačního systému.

Při příštím spuštění aplikace ověří součást aplikace Kaspersky Endpoint Security integritu aplikace. Pokud je aplikace nezměněná, součást pro ni použije aktuální oprávnění aplikací. Pokud došlo ke změně aplikace, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spouštěna poprvé.

Nastavení součásti Prevence narušení hostitele

Parametr	Popis
Oprávnění aplikací	**Aplikace** Tabulka aplikací, které jsou sledovány součástí Prevence narušení hostitele. Aplikace jsou přiřazovány do skupin důvěryhodnosti. Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace. Můžete vybrat aplikaci z jednotného seznamu všech aplikací nainstalovaných v počítačích pod vlivem zásady a přidat aplikaci do skupiny důvěryhodnosti. Přístupová práva k aplikacím jsou uvedena v následujících tabulkách: • **Soubory a systémový registr**. Tato tabulka obsahuje práva aplikací ve skupině důvěry pro přístup k prostředkům operačního systému a osobním datům. • **Práva**. Tento sloupec práva aplikací ve skupině důvěry k přístupu k procesům a prostředkům operačního systému. • **Pravidla sítě**. Tabulka síťových pravidel pro aplikace, které jsou součástí skupiny důvěryhodnosti. V souladu s těmito pravidly brána firewall reguluje síťovou aktivitu aplikací. Tabulka uvádí předdefinovaná pravidla sítě, která doporučují odborníci společnosti Kaspersky. Tato pravidla sítě byla přidána k optimální ochraně síťového provozu počítačů s operačními systémy Windows. Předdefinovaná pravidla sítě nelze odstranit.
Chráněné prostředky	**Název** Tabulka obsahuje kategorizované počítačové prostředky. Součást Prevence narušení hostitele sleduje pokusy jiných aplikací o přístup k prostředkům v tabulce. Prostředek může být kategorie registru, soubor, složka nebo klíč registru. **Aplikace** Tabulka aplikací sledovaných součástí Prevence narušení hostitele pro vybraný zdroj. Aplikace jsou přiřazovány do skupin důvěryhodnosti. Skupina důvěryhodnosti definuje oprávnění, na která aplikace Kaspersky Endpoint Security odkazuje při kontrole činnosti aplikace.
Skupina	

důvěryhodnosti pro aplikace spuštěné před spuštěním aplikace Kaspersky Endpoint Security	Skupina důvěryhodnosti, do které aplikace Kaspersky Endpoint Security umísťuje aplikace spuštěné před touto aplikací.
Aktualizovat práva pro dříve neznámé aplikace z databáze služby KSN	Pokud je toto políčko zaškrtnuto, bude součást Prevence narušení hostitele aktualizovat práva pro dříve neznámé aplikace pomocí databáze Služby hodnocení reputace KSN.
Důvěřovat aplikacím s digitálním podpisem	Pokud je toto políčko zaškrtnuto, umístí součást Prevence narušení hostitele aplikace s digitálním podpisem důvěryhodných dodavatelů do skupiny Důvěryhodné. *Důvěryhodní dodavatelé* jsou ti dodavatelé softwaru, kterým společnost Kaspersky důvěřuje. Certifikát dodavatele můžete také přidat do úložiště důvěryhodných certifikátů ručně. Jestliže je zaškrtnutí tohoto políčka zrušeno, nebude součást Prevence narušení hostitele považovat takovéto aplikace za důvěryhodné a použije k určení jejich skupiny důvěryhodnosti jiné parametry.
Odstranit oprávnění u aplikací, které nebyly spuštěny déle než N dní	Je-li zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security automaticky odstraní informace o aplikaci (skupina důvěryhodnosti a přístupová práva), jestliže jsou splněny následující podmínky: • Aplikaci jste ručně vložili do skupiny důvěryhodnosti nebo nakonfigurovali její přístupová práva. • Aplikace nebyla spuštěna v definovaném časovém období. Pokud byly skupina důvěryhodnosti a oprávnění aplikace stanoveny automaticky, aplikace Kaspersky Endpoint Security odstraní informace o této aplikaci po 30 dnech. Není možné změnit dobu uložení informací o aplikaci ani vypnout automatické odstranění. Při příštím spuštění této aplikace ji aplikace Kaspersky Endpoint Security analyzuje, jako by byla spuštěna poprvé.
Skupina důvěryhodnosti pro aplikace, které nelze přiřadit k jiným skupinám	Aplikace Kaspersky Endpoint Security na základě položky vybrané v tomto rozevíracím seznamu určí, do které skupiny důvěryhodnosti bude neznámá aplikace zařazena. Máte na výběr tyto položky: • **Nízké omezení**. • **Vysoké omezení**. • **Nedůvěryhodné**.

Modul pro nápravu

Součást Modul pro nápravu umožňuje aplikaci Kaspersky Endpoint Security vrátit zpět akce, které byly provedeny malwarem v operačním systému.

Při vracení změn provedených malwarem v operačním systému zpracuje aplikace Kaspersky Endpoint Security následující typy činností malwaru:

- **Činnost prováděná se soubory**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Odstraní spustitelné soubory, které byly vytvořeny malwarem (na všech médiích kromě síťových jednotek).
  - Odstraní spustitelné soubory, které byly vytvořeny programy, do nichž pronikl malware.
  - Obnoví soubory, které byly upraveny nebo odstraněny malwarem.

  Funkce obnovení souborů obsahuje řadu omezení.

- **Činnost prováděná v registru**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Odstraní klíče registru, které byly vytvořeny malwarem.
  - Neobnoví klíče registru, které byly upraveny nebo odstraněny malwarem.

- **Činnost systému**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Ukončí procesy, které byly zahájeny malwarem.
  - Ukončí procesy, do nichž pronikla nějaká škodlivá aplikace.
  - Neobnoví procesy, které byly zastaveny malwarem.

- **Síťová aktivita**

  Aplikace Kaspersky Endpoint Security provede následující akce:

  - Blokuje síťovou aktivitu malwaru.
  - Blokuje síťovou aktivitu procesů, do nichž pronikl malware.

Vrácení akcí malwaru může být zahájeno součástí Ochrana před souborovými hrozbami nebo Detekce chování nebo během antivirové kontroly.

Vrácení změn provedených malwarem má vliv na striktně definovanou sadu dat. Vrácení změn nemá žádný nežádoucí vliv na operační systém ani na integritu dat počítače.

Služba hodnocení reputace KSN

Aby mohla aplikace Kaspersky Endpoint Security chránit váš počítač efektivněji, využívá data přijatá od uživatelů po celém světě. Pro přijímání těchto dat je určena služba Kaspersky Security Network.

Služba Kaspersky Security Network (KSN) představuje infrastrukturu cloudových služeb, která poskytuje přístup k internetové znalostní bázi společnosti Kaspersky s informacemi o reputaci souborů, webových prostředcích a softwaru. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikace Kaspersky Endpoint Security na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků. Jestliže se účastníte služby Kaspersky Security Network, služby KSN poskytují aplikaci Kaspersky Endpoint Security informace o kategorii a pověsti naskenovaných souborů a také informace o pověsti kontrolovaných webových adres.

Používání služby hodnocení reputace Kaspersky Security Network je dobrovolné. Aplikace vás vyzve k použití služby KSN během úvodní konfigurace aplikace. Uživatel může účast v programu KSN zahájit nebo ukončit kdykoli.

Podrobnější informace o statistických informacích generovaných při účasti v síti KSN, které jsou odesílány společnosti Kaspersky, a o uchovávání a likvidaci těchto informací najdete v prohlášení o službě Kaspersky Security Network a na webových stránkách společnosti Kaspersky. Soubor ksn_<ID jazyka>.txt s textem prohlášení o službě Kaspersky Security Network je součástí distribučního balíčku aplikace.

Za účelem snížení zatížení serverů služby KSN může společnost Kaspersky vydat aktualizace aplikace, které dočasně deaktivují nebo částečně omezí odesílání požadavků do služby Kaspersky Security Network. V tomto případě je stav připojení ke KSN v místním rozhraní aplikace *Povoleno s omezeními*.

Infrastruktura KSN

Aplikace Kaspersky Endpoint Security podporuje následující řešení infrastruktury KSN:

- *Globální KSN* je řešení, které používá většina aplikací Kaspersky. Účastníci služby Kaspersky Security Network získávají z této služby informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází pověsti a statistik služby Kaspersky Security Network.

- *Privátní KSN* je řešení, které umožňuje uživatelům počítačů, které jsou hostiteli aplikace Kaspersky Endpoint Security nebo jiných aplikací společnosti Kaspersky, získat přístup k databázím pověsti služby Kaspersky Security Network a k dalším statistickým údajům bez odesílání dat do KSN z vlastních počítačů. Možnost privátní KSN je určena pro firemní zákazníky, kteří nemohou být součástí služby Kaspersky Security Network z některého z následujících důvodů:

  - Místní pracovní stanice nejsou připojeny k internetu.

  - Přenos jakýchkoli dat mimo zemi nebo mimo podnikovou síť LAN je zakázán zákonem nebo je omezen firemními bezpečnostními zásadami.

Ve výchozím nastavení aplikace Kaspersky Security Center používá globální KSN. Použití privátní služby KSN můžete nakonfigurovat v konzole pro správu (MMC) a webové konzole aplikace Kaspersky Security Center 12 a na příkazovém řádku. V cloudové konzole aplikace Kaspersky Security Center nelze součást používání privátní KSN konfigurovat.

Více informací o privátní KSN naleznete v *dokumentaci k aplikaci Kaspersky Private Security Network*.

Proxy server KSN

Uživatelské počítače spravované administračním serverem Kaspersky Security Center mohou se sítí KSN komunikovat prostřednictvím služby proxy serveru KSN.

Služba proxy serveru KSN poskytuje následující možnosti:

- Počítač uživatele může odesílat dotazy a informace do služby KSN i bez přímého přístupu k internetu.
- Služba proxy serveru KSN ukládá zpracovaná data do mezipaměti, čímž snižuje zatížení komunikačního kanálu a externí sítí a urychluje příjem informací, které jsou uživatelským počítačem požadovány.

Další informace o službě proxy serveru KSN najdete v *průvodci nápovědou k aplikaci Kaspersky Security Center*.

Nastavení služby Kaspersky Security Network

Parametr	Popis
Povolit rozšířený režim KSN	*Rozšířený režim služby KSN* je režim, ve kterém aplikace Kaspersky Endpoint Security odesílá společnosti Kaspersky více údajů. Aplikace Kaspersky Endpoint Security používá službu KSN k detekci hrozeb bez ohledu na pozici přepínače.
Povolit režim cloudu	*Cloudový režim* znamená režim provozu aplikace, ve kterém Kaspersky Endpoint Security používá neúplnou verzi antivirových databází. Když se používají neúplné antivirové databáze, aplikace Kaspersky Security Network podporuje provoz aplikace. Neúplná verze antivirových databází vám umožňuje využívat přibližně polovinu paměti RAM počítače, která by se jinak využívala u obvyklých databází. Pokud se neúčastníte služby Kaspersky Security Network nebo pokud je cloudový režim vypnutý, Kaspersky Endpoint Security stáhne plnou verzi antivirových databází ze serverů společnosti Kaspersky. Pokud je přepínací tlačítko v zapnuté poloze, bude aplikace Kaspersky Endpoint Security používat neúplnou verzi antivirových databází, čímž sníží nároky na prostředky operačního systému. Po zaškrtnutí tohoto políčka stáhne aplikace Kaspersky Endpoint Security neúplnou verzi antivirových databází při další aktualizaci. Pokud je přepínací tlačítko ve vypnuté poloze, bude aplikace Kaspersky Endpoint Security používat úplnou verzi antivirových databází. Po zrušení zaškrtnutí tohoto políčka stáhne aplikace Kaspersky Endpoint Security úplnou verzi antivirových databází při další aktualizaci.
Stav počítače v případě nedostupnosti serverů KSN *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Položky v tomto rozevíracím seznamu určují stav počítače ve službě Kaspersky Security Center v případě, že servery služby KSN nejsou dostupné.
Použít proxy server KSN	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije službu proxy serveru KSN. Nastavení služby proxy serveru KSN můžete nakonfigurovat ve vlastnostech serveru pro správu.

(k dispozici pouze v konzole aplikace Kaspersky Security Center)	
Použít servery KSN, pokud není KSN Proxy k dispozici *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Pokud je zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security použije servery KSN v případě nedostupnosti služby proxy serveru KSN. Servery KSN mohou být umístěny na straně společnosti Kaspersky (při použití globální KSN) a u třetí strany (při použití privátní KSN).

Kontrola webu

Kontrola webu řídí přístup uživatelů k webovým prostředkům. To pomáhá omezit provoz a nevhodné využití pracovní doby. Když se uživatel pokusí otevřít web, k němuž omezuje přístup součást Kontrola webu, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).

Aplikace Kaspersky Endpoint Security sleduje pouze provoz HTTP a HTTPS.

Pro sledování provozu HTTPS je třeba povolit kontroly šifrovaných připojení.

Metody pro správu přístupu k webům

Kontrola webu umožňuje konfigurovat přístup k webům následujícími způsoby:

- **Kategorie webu**. Weby jsou tříděny podle cloudové služby Kaspersky Security Network, heuristické analýzy a databáze známých webů (jedna z databází aplikace). Můžete například omezit přístup uživatelů ke kategorii „Sociální sítě“ nebo jiným kategoriím.
- **Typ dat**. Můžete omezit přístup uživatelů k datům na webu a skrýt například grafické obrázky. Aplikace Kaspersky Endpoint Security určuje typ dat na základě formátu souboru, a ne na základě jeho přípony.

  Aplikace Kaspersky Endpoint Security nekontroluje soubory v archivech. Pokud byly například obrazové soubory umístěny do archivu, aplikace Kaspersky Endpoint Security identifikuje datový typ „Archivy“, nikoli „Grafické soubory“.

- **Jednotlivé adresy**. Můžete zadat webovou adresu nebo použít masky.

Pro regulaci přístupu na webové stránky můžete současně použít několik způsobů. Můžete například omezit přístup ke kategorii webu „Soubory sady Office“ pouze pro kategorii webových stránek „Webový e-mail“.

Pravidla přístupu k webu

Součást Kontrola zařízení řídí přístup uživatelů k zařízením pomocí *pravidel přístupu*. Pro pravidlo přístupu k webu můžete nakonfigurovat následující rozšířená nastavení:

- Uživatelé, na které se pravidlo vztahuje.

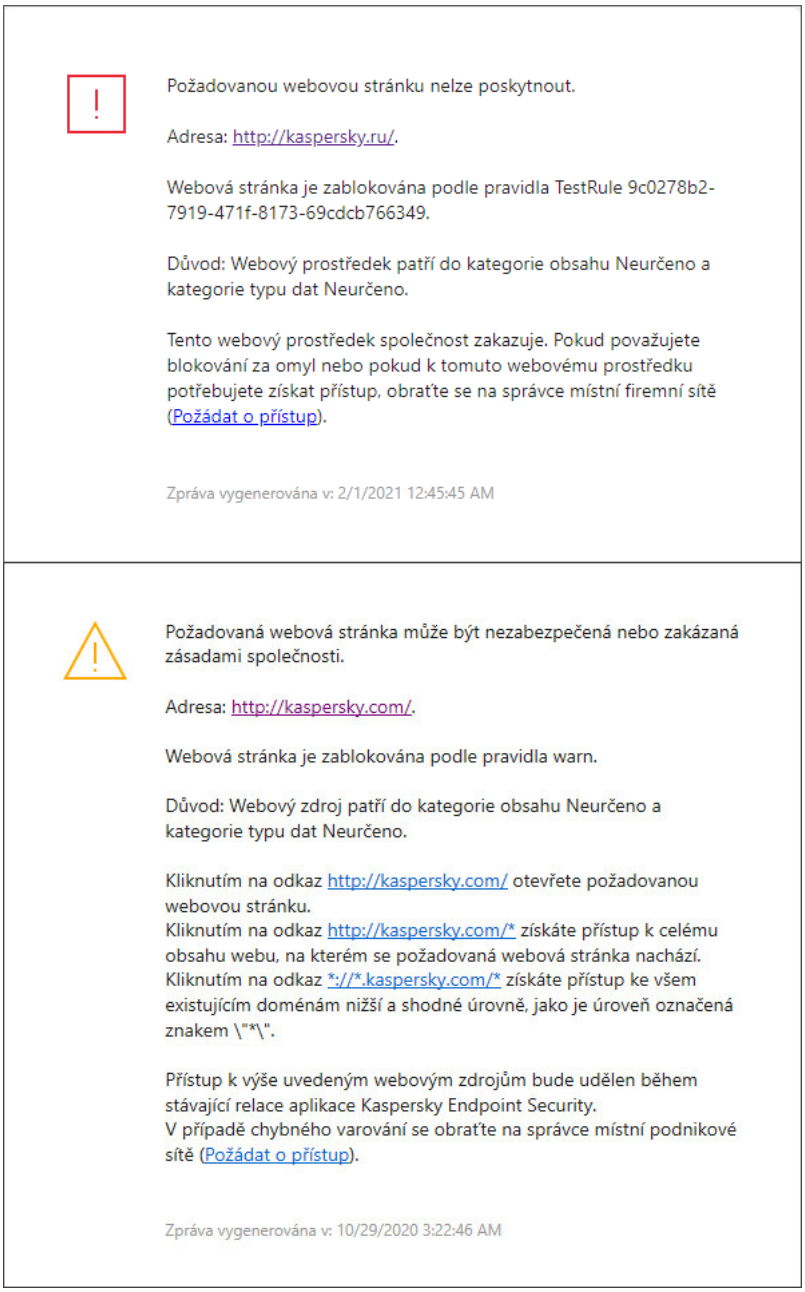
  Můžete například omezit přístup k internetu prostřednictvím prohlížeče pro všechny uživatele společnosti kromě IT oddělení.

- Plán pravidel.

  Můžete například omezit přístup k internetu prostřednictvím prohlížeče pouze v pracovní době.

Priority pravidel přístupu

Každé pravidlo má prioritu. Čím výše se pravidlo na seznamu nachází, tím vyšší je jeho priorita. Pokud byl web přidán do více pravidel, řídí součást Kontrola webu přístup k webu na základě pravidla s nejvyšší prioritou. Aplikace Kaspersky Endpoint Security může například identifikovat firemní portál jako sociální síť. Chcete-li omezit přístup k sociálním sítím a poskytnout přístup k firemnímu webovému portálu, vytvořte dvě pravidla: jedno pravidlo blokující kategorii webových stránek „Sociální sítě“ a jedno pravidlo povolující firemní webový portál. Pravidlo přístupu pro firemní webový portál musí mít vyšší prioritu než pravidlo přístupu pro sociální sítě.



Zprávy součástí Kontrola webu

Nastavení součásti Kontrola webu

Parametr	Popis
Pravidla přístupu k webovým prostředkům	Seznam obsahující pravidla přístupu k webovým prostředkům. Každé pravidlo má prioritu. Čím výše se pravidlo na seznamu nachází, tím vyšší je jeho priorita. Pokud byl web přidán do více pravidel, řídí součást Kontrola webu přístup k webu na základě pravidla s nejvyšší prioritou.
Výchozí pravidlo	*Výchozí pravidlo* je pravidlo přístupu k webovým prostředkům, na které se nevztahuje žádné jiné pravidlo. K dispozici jsou následující možnosti: • **Povolit vše kromě seznamu pravidel**, známý také jako režim zakázaných webů. • **Zakázat vše kromě seznamu pravidel**, známý také jako režim povolených webů.
Šablony zpráv	• **Varování**. Pole pro zadání zahrnuje šablony zprávy, která se zobrazí, pokud je aktivováno pravidlo varování o pokusech o přístup k nežádoucímu webovému prostředku.

	• **Zpráva o blokování**. Pole pro zadání obsahuje šablonu zprávy, která se zobrazí, pokud je aktivováno pravidlo, které blokuje přístup k webovému prostředku. • **Zpráva správci**. Pole pro zadání obsahuje šablonu zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem.
Protokolovat otvírání povolených stránek	Aplikace Kaspersky Endpoint Security protokoluje data při návštěvách všech webů, včetně povolených. Kaspersky Endpoint Security odesílá události do aplikace Kaspersky Security Center, do místního protokolu aplikace Kaspersky Endpoint Security a do protokolu událostí systému Windows. Chcete-li sledovat aktivitu uživatele na internetu, musíte nakonfigurovat nastavení pro ukládání událostí. Sledování aktivity uživatele na internetu může vyžadovat více prostředků počítače při dešifrování provozu HTTPS.

Kontrola zařízení

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Kontrola zařízení spravuje přístup uživatelů k zařízením, která jsou nainstalována v počítači nebo jsou k němu připojena (například pevné disky, fotoaparáty nebo moduly Wi-Fi). Díky tomu můžete chránit počítač před nakažením, když jsou taková zařízení připojena, a zabránit ztrátě nebo úniku dat.

Úrovně přístupu k zařízení

Součást Kontrola zařízení řídí přístup na následujících úrovních:

- **Typ zařízení**. Například zařízení, vyměnitelné jednotky a jednotky CD/DVD.
  Přístup k zařízení můžete nakonfigurovat následujícím způsobem:
  - Povolit – ✓.
  - Blokovat – ⊘.
  - Závisí na sběrnici připojení (kromě sítě Wi-Fi) – .
  - Blokovat s výjimkami (pouze Wi-Fi) – .
- **Sběrnice připojení**. *Sběrnice připojení* je rozhraní, které slouží k připojení zařízení k počítači (například rozhraní USB nebo FireWire). Můžete tedy omezit připojení všech zařízení, například přes port USB.
  Přístup k zařízení můžete nakonfigurovat následujícím způsobem:
  - Povolit – ✓.
  - Blokovat – ⊘.

- **Důvěryhodná zařízení**. *Důvěryhodná zařízení* jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

  Důvěryhodná zařízení můžete přidat na základě následujících dat:

  - **Zařízení dle ID**. Každé zařízení má jedinečný identifikátor (ID hardwaru neboli HWID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Příklad ID zařízení: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Přidání zařízení podle ID je praktické, když chcete přidat několik konkrétních zařízení.

  - **Zařízení dle modelu**. Každé zařízení má ID dodavatele (VID) a ID produktu (PID). ID můžete zobrazit ve vlastnostech zařízení pomocí nástrojů operačního systému. Šablona pro zadání VID a PID: `VID_1234&PID_5678`. Přidání zařízení podle modelu je praktické, pokud v organizaci používáte zařízení určitého modelu. Tímto způsobem můžete přidat všechna zařízení tohoto modelu.

  - **Zařízení dle masky ID**. Pokud používáte více zařízení s podobnými ID, můžete je přidat do seznamu důvěryhodných zařízení pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `WDC_C *`.

  - **Zařízení dle masky modelu**. Pokud používáte více zařízení s podobnými VID nebo PID (například zařízení od stejného výrobce), můžete přidat zařízení na seznam důvěryhodných pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `VID_05AC & PID_*`.

Součást Kontrola zařízení reguluje přístup uživatele k zařízením pomocí *pravidel přístupu*. Součást Kontrola zařízení umožňuje také uložit události připojení/odpojení zařízení. Chcete-li uložit události, je třeba nakonfigurovat registraci událostí do zásady.

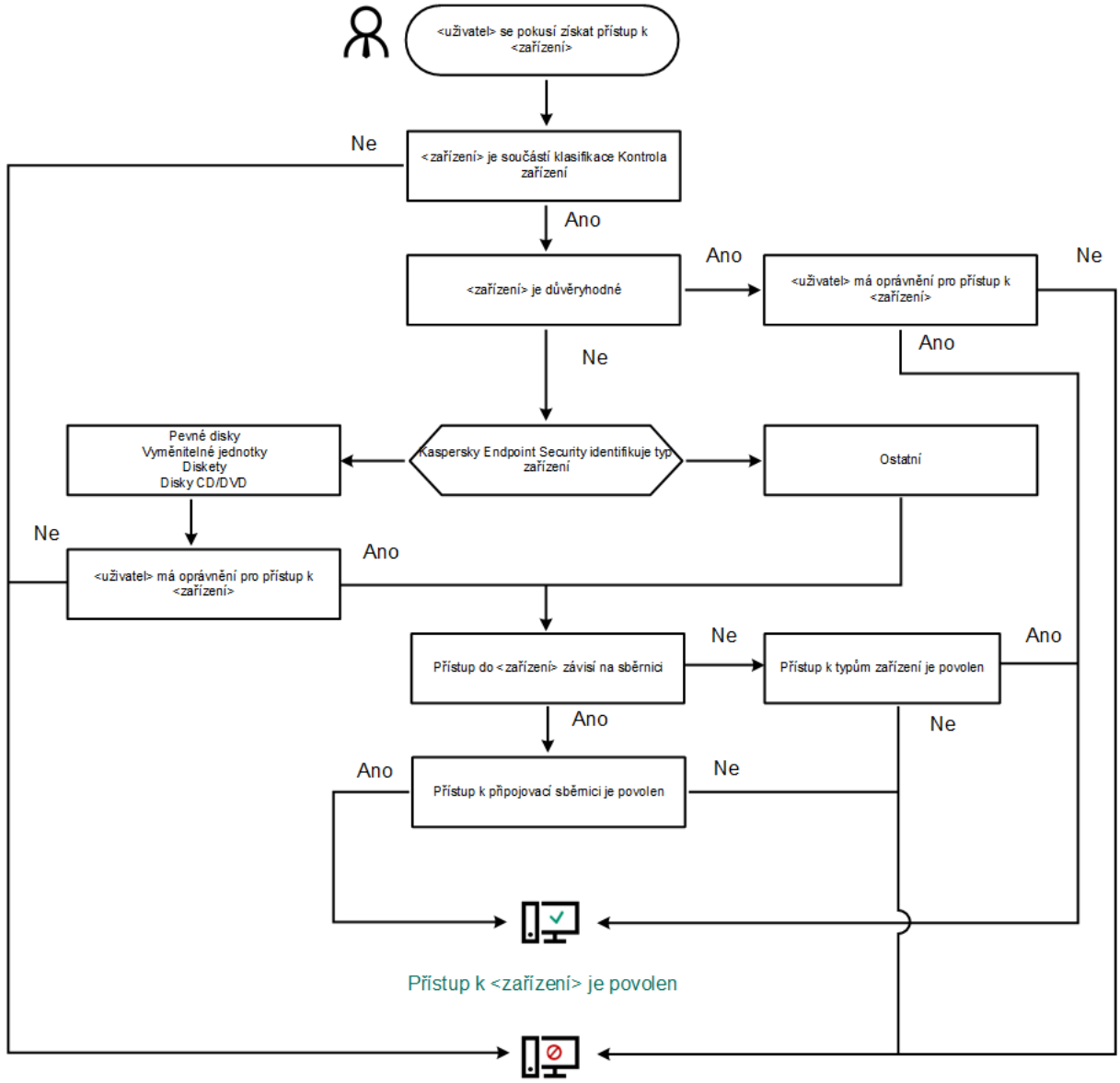
Pokud přístup k zařízení závisí na sběrnici připojení (stav), aplikace Kaspersky Endpoint Security neuloží události připojení/odpojení zařízení. Chcete-li aplikaci Kaspersky Endpoint Security umožnit, aby uložila události připojení/odpojení zařízení, povolte přístup k odpovídajícímu typu zařízení (stav) nebo přidejte zařízení do seznamu důvěryhodných zařízení.

Když je k počítači připojeno zařízení, které je blokováno součástí Kontrola zařízení, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).

Upozornění součásti Kontrola zařízení

Algoritmus činnosti součásti Kontrola zařízení

Aplikace Kaspersky Endpoint Security rozhoduje o tom, zda povolit přístup k zařízení poté, co ho uživatel připojí k počítači (viz obrázek níže).



Algoritmus činnosti součásti Kontrola zařízení

Pokud je zařízení připojeno a přístup je povolen, můžete upravit pravidlo přístupu a přístup blokovat. V takovém případě aplikace Kaspersky Endpoint Security při příštím pokusu o přístup k zařízení (například zobrazení stromu složek nebo provedení operace čtení nebo zápisu) zablokuje přístup. Zařízení bez souborového systému bude zablokováno až při příštím připojení zařízení.

Pokud musí uživatel počítače s nainstalovanou aplikací Kaspersky Endpoint Security zažádat o přístup k zařízení, o kterém si myslí, že je blokováno neopodstatněně, zašlete uživateli pokyny k vyžádání přístupu.

Nastavení součásti Kontrola zařízení

Parametr	Popis
Povolit žádosti o dočasný přístup *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Je-li toto políčko zaškrtnuto, tlačítko **Požádat o přístup** bude dostupné prostřednictvím místního rozhraní aplikace Kaspersky Endpoint Security. Kliknutím na toto tlačítko otevřete okno **Požádat o přístup k zařízení**. V tomto okně může uživatel požádat o dočasný přístup k zablokovanému zařízení.

Zařízení a Wi-Fi sítě	Tato tabulka obsahuje všechny možné typy zařízení dle klasifikace součásti Kontrola zařízení, včetně jejich příslušného stavu přístupu.
Sběrnice připojení	Seznam všech dostupných sběrnic připojení dle klasifikace součásti Kontrola zařízení, včetně jejich příslušného stavu přístupu.
Důvěryhodná zařízení	Seznam důvěryhodných zařízení a uživatelů, kterým byl udělen přístup k těmto zařízením.
Anti-Bridging	Anti-Bridging zamezuje vytváření síťových mostů tím, že brání tomu, aby se v počítači současně vytvářelo více síťových připojení. To vám umožní chránit podnikovou síť před útoky přes nechráněné nepovolané sítě. Anti-Bridging blokuje vytváření více připojení podle priorit zařízení. Čím výše se zařízení na seznamu nachází, tím vyšší je jeho priorita. Jsou-li aktivní i nové připojení stejného typu (například Wi-Fi), aplikace Kaspersky Endpoint Security zablokuje aktivní připojení a umožňuje navázání nového připojení. Jsou-li aktivní a nové připojení různého typu (například síťový adaptér a Wi-Fi), aplikace Kaspersky Endpoint Security zablokuje připojení s nižší prioritou a umožní připojení s vyšší prioritou. Anti-Bridging podporuje provoz následujících typů zařízení: síťový adaptér, Wi-Fi a modem.
Šablony zpráv	• **Zpráva o blokování**. Šablona zprávy, která se zobrazí, když se uživatel pokusí o přístup k blokovanému zařízení. Tato zpráva se také zobrazí, když se uživatel pokusí provést činnost s obsahem zařízení, které bylo pro tohoto uživatele zablokováno. • **Zpráva správci**. Šablona zprávy, která bude odeslána správci sítě LAN, když se uživatel domnívá, že přístup k zařízení byl zablokován omylem nebo že činnosti s obsahem zařízení jsou nedopatřením zakázány.

Kontrola aplikací

Součást Kontrola aplikací řídí spouštění aplikací v počítačích uživatelů. Tím vám umožňuje implementovat podnikové zásady zabezpečení při používání aplikací. Součást Kontrola aplikací také snižuje riziko počítačové infekce omezením přístupu k aplikacím.

Konfigurace součásti Kontrola aplikací se skládá z následujících kroků:

1. Vytvoření kategorií aplikací.

   Správce vytvoří kategorie aplikací, které chce spravovat. Kategorie aplikací jsou určeny pro všechny počítače v podnikové síti bez ohledu na skupiny pro správu. Chcete-li vytvořit kategorii, můžete použít následující kritéria: Kategorie KL (například *Prohlížeče*), hodnota hash souboru, dodavatel aplikace a další kritéria.

2. Vytvoření pravidel součásti Kontrola aplikací.

   Správce vytvoří pravidla součástí Kontrola aplikací v zásadách pro skupinu správy. Pravidlo zahrnuje kategorie aplikace a stav spouštění aplikací z těchto kategorií: blokované nebo povolené.

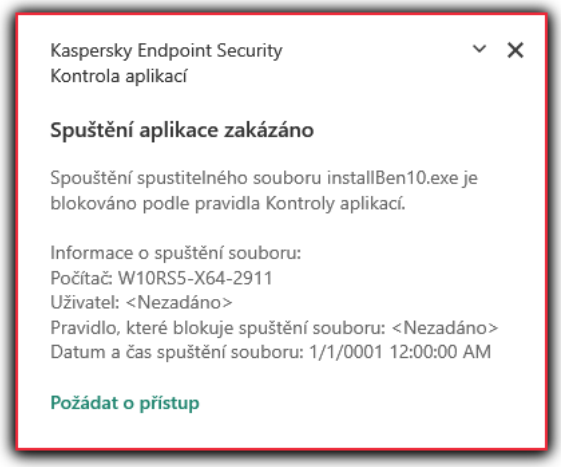
3. Volba režimu součásti Kontrola aplikací.

Správce vybere režim pro práci s aplikacemi, které nejsou zahrnuty v žádném z pravidel (seznam blokovaných aplikací nebo seznam povolených aplikací).

Pokud se uživatel pokusí spustit zakázanou aplikaci, aplikace Kaspersky Endpoint Security její spuštění zablokuje a zobrazí upozornění (viz obrázek níže).

K dispozici je *testovací režim* pro kontrolu konfigurace součásti Kontrola aplikací. V tomto režimu aplikace Kaspersky Endpoint Security provádí následující akce:

- Umožňuje spouštění aplikací, včetně těch zakázaných.
- Zobrazuje oznámení o spuštění zakázané aplikace a přidá informace do zprávy v počítači uživatele.
- Odesílá data o spuštění zakázaných aplikací do aplikace Kaspersky Security Center.



Upozornění součásti Kontrola aplikací

Režimy operace součásti Kontrola aplikací

Součást Kontrola aplikací funguje ve dvou režimech:

- **Seznam blokovaných položek**. V tomto režimu umožňuje Kontrola aplikací uživatelům spouštět všechny aplikace kromě aplikací, které jsou v jejích pravidlech zakázány.

  Tento režim je ve výchozím nastavení povolen.

- **Seznam povolených položek**. V tomto režimu neumožňuje Kontrola aplikací uživatelům spouštět všechny aplikace kromě aplikací, které jsou v jejích pravidlech povoleny a nejsou zakázány.

  Pokud jsou pravidla povolených aplikací součástí Kontrola aplikací plně nakonfigurována, tato součást blokuje spouštění všech nových aplikací, které nebyly ověřeny správcem LAN, a zároveň umožňuje fungování operačního systému a důvěryhodných aplikací, které uživatelé potřebují pro práci.

  Můžete si přečíst doporučení ohledně konfigurace pravidel součásti Kontrola aplikací v režimu povolených aplikací.

Součást Kontrola aplikací lze nakonfigurovat tak, aby v těchto režimech fungovala jak pomocí místního rozhraní aplikace Kaspersky Endpoint Security, tak pomocí aplikace Kaspersky Security Center.

Aplikace Kaspersky Security Center však nabízí nástroje, které nejsou dostupné v místním rozhraní aplikace Kaspersky Endpoint Security, jako jsou například nástroje potřebné pro následující úkoly:

- Vytvoření kategorií aplikací.

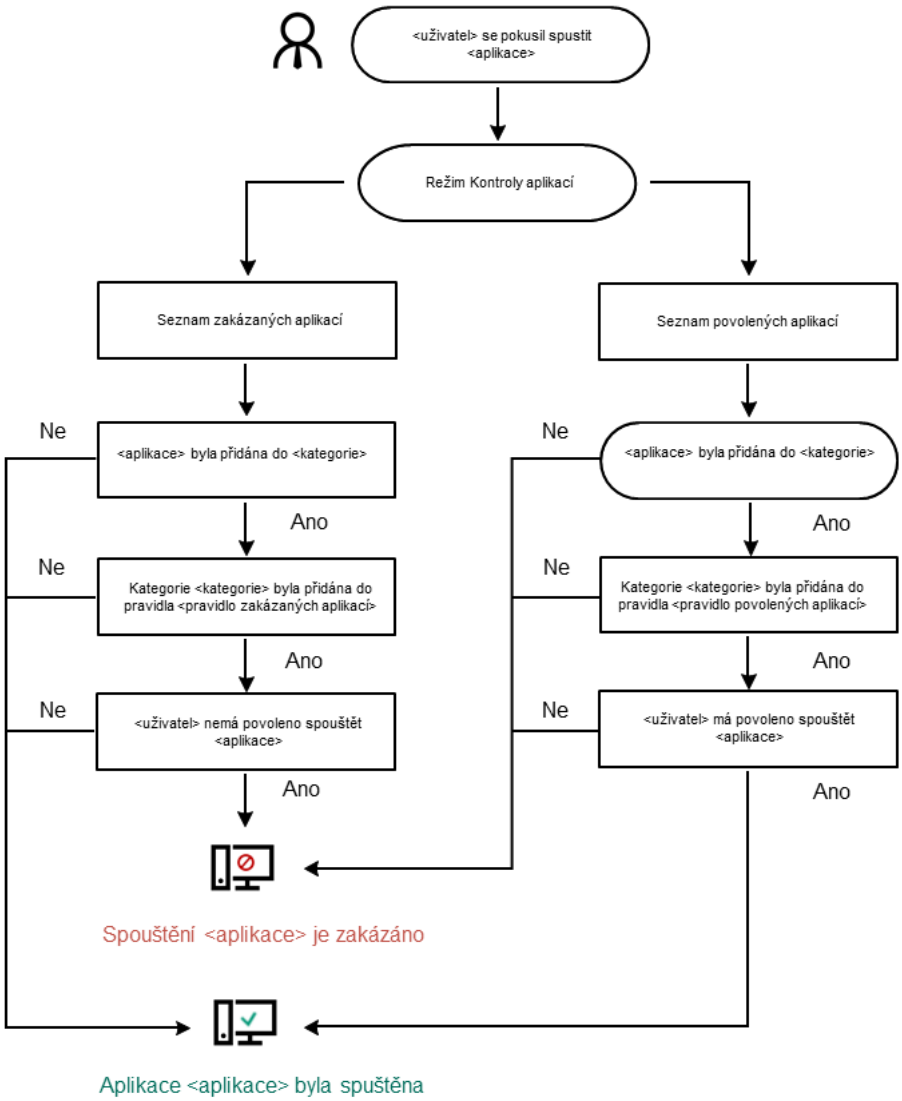
Pravidla součásti Kontrola aplikací vytvořená v konzole pro správu aplikace Kaspersky Security Center jsou založena na vašich vlastních kategoriích aplikací, nikoli na podmínkách zahrnutí a vyloučení, jako je tomu v místním rozhraní aplikace Kaspersky Endpoint Security.

- Získávání informací o aplikacích nainstalovaných v počítačích v podnikové síti LAN.

Z tohoto důvodu se doporučuje používat aplikaci Kaspersky Security Center ke konfiguraci provozu součásti Kontrola aplikací.

Algoritmus činnosti součásti Kontrola aplikací

Aplikace Kaspersky Endpoint Security používá k rozhodnutí o spuštění aplikace algoritmus (viz obrázek níže).



Algoritmus činnosti součásti Kontrola aplikací

Nastavení součásti Kontrola aplikací

Parametr	Popis
Testovací režim	Pokud je přepínací tlačítko v zapnuté poloze, povolí aplikace Kaspersky Endpoint Security spuštění aplikace, která je v aktuálním režimu součásti Kontrola aplikací zablokována, ale

	zaznamená informace o jejím spuštění do zprávy protokolu.
Režim Kontroly aplikací	Máte na výběr tyto možnosti: • **Seznam blokovaných položek**. Pokud je vybrána tato možnost, umožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel blokování součásti Kontrola aplikací. • **Seznam povolených položek**. Pokud je vybrána tato možnost, znemožní součást Kontrola aplikací všem uživatelům spouštět libovolné aplikace s výjimkou případů, kdy aplikace splňuje podmínky pravidel povolení součásti Kontrola aplikací. Při výběru režimu **Seznam povolených položek** jsou automaticky vytvořena dvě pravidla součásti Kontrola aplikací: • **Golden Image**. • **Důvěryhodné nástroje aktualizace**. Automaticky vytvořená pravidla nemůžete odstranit ani upravovat jejich nastavení. Tato pravidla můžete povolit nebo zakázat.
Kontrola DLL	Je-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security kontroluje načítání modulů DLL, když se uživatel pokusí o spuštění aplikací. Informace o modulu DLL a aplikaci, která tento modul DLL načetla, jsou zaprotokolovány do zprávy. Při povolování kontroly načítání modulů DLL a ovladačů se ujistěte, že je v nastavení oddílu Kontrola aplikací povoleno jedno z následujících pravidel: výchozí pravidlo **Golden Image** nebo jiné pravidlo, které obsahuje kategorii KL „Důvěryhodné certifikáty“ a zajišťuje načtení důvěryhodných modulů DLL a ovladačů před spuštěním aplikace Kaspersky Endpoint Security. Povolení řízení načítání modulů DLL a ovladačů v případě zakázání pravidla **Golden Image** může způsobit nestabilitu v operačním systému. Aplikace Kaspersky Endpoint Security monitoruje pouze moduly DLL a ovladače načtené od okamžiku zaškrtnutí políčka. Po zaškrtnutí tohoto políčka se doporučuje restartovat počítač, aby se zajistilo, že aplikace sleduje všechny moduly a ovladače DLL, včetně těch, které byly načteny před spuštěním aplikace Kaspersky Endpoint Security.
Šablony zpráv	**Zpráva o blokování**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace. **Zpráva správci**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

Adaptivní kontrola anomálií

Tato součást je k dispozici pouze pro aplikace Kaspersky Endpoint Security for Business Advanced a Kaspersky Total Security for Business. Podrobnější informace o aplikaci Kaspersky Endpoint Security for Business najdete na *webu společnosti Kaspersky*.

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Součást Adaptivní kontrola anomálií sleduje a blokuje akce, které nejsou obvyklé pro počítače v podnikové síti. Adaptivní kontrola anomálií používá ke sledování necharakteristického chování sadu pravidel (například pravidlo *Spuštění prostředí Microsoft PowerShell z aplikace sady Office*). Pravidla vytvářejí odborníci společnosti Kaspersky na základě typických scénářů škodlivé činnosti. Můžete nakonfigurovat, jak součást Adaptivní kontrola anomálií zpracovává každé pravidlo, a povolit například provádění skriptů PowerShell, které automatizují určité úlohy pracovního postupu. Aplikace Kaspersky Endpoint Security aktualizuje sadu pravidel spolu s databázemi aplikací. Aktualizace sad pravidel musí být potvrzeny ručně.

Nastavení součásti Adaptivní kontrola anomálií

Konfigurace součásti Adaptivní kontrola anomálií se skládá z následujících kroků:

1. Zkušební režim součásti Adaptivní kontrola anomálií.

   Poté, co povolíte součást Adaptivní kontrola anomálií, její pravidla fungují ve *zkušebním režimu*. Ve zkušebního režimu monitoruje součást Adaptivní kontrola anomálií aktivaci pravidel a odesílá aktivační události do centra Kaspersky Security Center. Každé pravidlo má své vlastní trvání zkušebního režimu. Doba trvání zkušebního režimu je nastavena odborníky společnosti Kaspersky. Obvykle je zkušební režim aktivní dva týdny.

   Pokud není během zkušebního režimu nějaké pravidlo aktivováno vůbec, bude součást Adaptivní kontrola anomálií akce spojené s tímto pravidlem považovat za netypické. Aplikace Kaspersky Endpoint Security bude blokovat všechny akce spojené s tímto pravidlem.

   Pokud bylo během zkušebního režimu nějaké pravidlo aktivováno, aplikace Kaspersky Endpoint Security zaznamená události do protokolu zpráva o aktivaci pravidel a úložiště **aktivace pravidel v chytrém zkušebním režimu**.

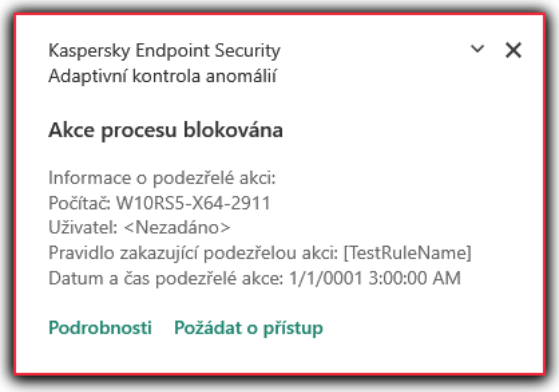
2. Analýza zprávy o aktivaci pravidel.

   Správce analyzuje zprávu o aktivaci pravidel nebo obsah úložiště **aktivace pravidel v chytrém zkušebním režimu**. Poté může správce zvolit chování součásti Adaptivní kontrola anomálií při aktivaci pravidla: blokovat nebo povolit. Správce může také sledovat, jak pravidlo funguje, a prodloužit dobu trvání zkušebního režimu. Pokud správce neprovede žádnou akci, aplikace bude i nadále fungovat ve zkušebním režimu. Doba zkušebního režimu začne běžet znovu.

Součást Adaptivní kontrola anomálií je konfigurována v reálném čase. Součást Adaptivní kontrola anomálií je konfigurována prostřednictvím následujících kanálů:

- Adaptivní kontrola anomálií automaticky začne blokovat akce spojené s pravidly, která nebyla nikdy spuštěna ve zkušebním režimu.
- Aplikace Kaspersky Endpoint Security přidává nová pravidla nebo odstraňuje zastaralá pravidla.
- Správce konfiguruje činnost součásti Adaptivní kontrola anomálií po kontrole zprávy o aktivaci pravidel a obsahu úložiště **aktivace pravidel v chytrém zkušebním režimu**. Doporučujeme zprávu o aktivaci pravidel a obsah úložiště **aktivace pravidel v chytrém zkušebním režimu kontrolovat**.

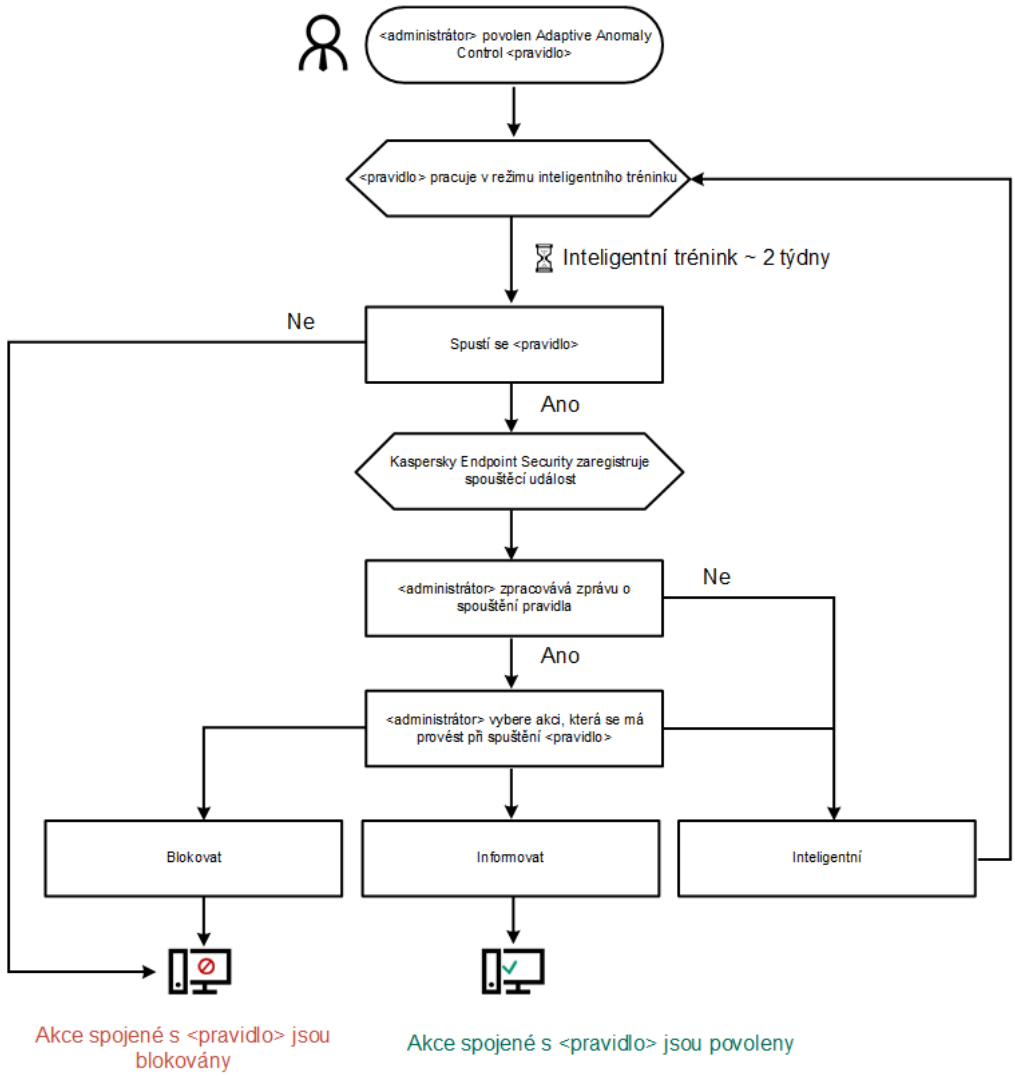
Pokud se škodlivá aplikace pokusí provést akci, aplikace Kaspersky Endpoint Security akci zablokuje a zobrazí upozornění (viz obrázek níže).



Oznámení součásti Adaptivní kontrola anomálií

Algoritmus činnosti součásti Adaptivní kontrola anomálií

Aplikace Kaspersky Endpoint Security určí, zda povolit nebo blokovat akci spojenou s pravidlem, na základě následujícího algoritmu (viz obrázek níže).



Algoritmus činnosti součásti Adaptivní kontrola anomálií

Nastavení součásti Adaptivní kontrola anomálií

Parametr	Popis
Zpráva o stavu pravidel	Tato zpráva obsahuje informace o stavu detekčních pravidel součásti Adaptivní kontrola anomálií (například *Vypnuto* nebo *Blokovat*). Zpráva je generována pro

(k dispozici pouze v konzole aplikace Kaspersky Security Center)	všechny skupiny pro správu.
Zpráva o aktivaci pravidel *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Tato zpráva obsahuje informace o netypických akcích zjištěných pomocí součásti Adaptivní kontrola anomálií. Zpráva je generována pro všechny skupiny pro správu.
Pravidla	Tabulka pravidel součásti Adaptivní kontrola anomálií. Pravidla vytvářejí odborníci společnosti Kaspersky na základě typických scénářů potenciálně škodlivé činnosti.
Šablony	• **Zpráva o blokování**. Šablona zprávy, která se zobrazí uživateli, když je spuštěno pravidlo součásti Adaptivní kontrola anomálií, které blokuje netypickou akci. • **Zpráva správci**. Šablona zprávy, kterou uživatel může zaslat správci místní podnikové sítě, pokud považuje blokování za chybu.

Endpoint Sensor

Endpoint Sensor není součástí aplikace Kaspersky Endpoint Security 11.4.0.

Součást Endpoint Sensor můžete spravovat ve webové konzole aplikace Kaspersky Security Center 12 a v konzole pro správu aplikace Kaspersky Security Center. V cloudové konzole aplikace Kaspersky Security Center nelze součást Endpoint Sensor spravovat.

Endpoint Sensor je součást platformy Kaspersky Anti Targeted Attack Platform. Platforma Kaspersky *Anti Targeted Attack Platform* je řešení navržené pro včasnou detekci sofistikovaných hrozeb, jako jsou cílené útoky, pokročilé perzistentní hrozby (APT), útoky nultého dne a další. Platforma Kaspersky Anti Targeted Attack Platform zahrnuje dva funkční bloky: Kaspersky Anti Targeted Attack (dále také „*KATA*“) a Kaspersky Endpoint Detection and Response (dále také „*KEDR*“). KEDR si můžete zakoupit samostatně. Podrobné informace o řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

Správa součásti Endpoint Sensor má následující omezení:

- Je-li v počítači nainstalována aplikace Kaspersky Endpoint Security verze 11.0.0 až 11.3.0, nastavení součást Endpoint Sensor můžete nakonfigurovat v zásadách. Další informace o konfiguraci nastavení součásti Endpoint Sensor pomocí zásad najdete v článcích nápovědy pro předchozí verze aplikace Kaspersky Endpoint Security.
- Je-li v počítači nainstalována aplikace Kaspersky Endpoint Security verze 11.4.0 a vyšší, nastavení součásti Endpoint Sensor nemůžete konfigurovat pomocí zásad.

Součást Endpoint Sensor je instalována v klientských počítačích. V těchto počítačích součást nepřetržitě sleduje procesy, aktivní síťová připojení a soubory, které byly upraveny. Součást Endpoint Sensor předává informace na server platformy KATA.

Funkce součásti je k dispozici v následujících operačních systémech:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64bitová verze);
- Windows Server 2012 Foundation / Standard / Enterprise (64bitová verze);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64bitová verze);
- Windows Server 2016 Essentials / Standard (64bitová verze).

Podrobné informace o fungování platformy KATA *najdete v průvodci nápovědou k platformě Kaspersky Anti Targeted Attack*.

Úplné šifrování disku

Můžete vybrat technologii šifrování: Kaspersky Disk Encryption nebo BitLocker Drive Encryption (dále označována zkráceně jako „technologie BitLocker“).

Kaspersky Disk Encryption

Po zašifrování systémových pevných disků se musí uživatel při příštím spuštění počítače ověřit prostřednictvím ověřovacího agenta a až poté jsou zpřístupněna data na pevných discích a načten operační systém. Tato akce vyžaduje zadání hesla tokenu nebo čipové karty připojené k počítači nebo uživatelského jména a hesla účtu ověřovacího agenta, který byl vytvořen správcem místní sítě pomocí úlohy *Správa účtů ověřovacího agenta*. Tyto účty jsou založené na účtech systému Microsoft Windows, které uživatelé používají k přihlašování do operačního systému. Můžete také použít technologii SSO (Single Sign-On), která umožňuje automatické přihlášení k operačnímu systému pomocí uživatelského jména a hesla účtu ověřovacího agenta.

Ověření uživatele ověřovacím agentem lze provést dvěma způsoby:

- Zadejte název a heslo účtu ověřovacího agenta, který byl vytvořen správcem sítě LAN pomocí nástrojů aplikace Kaspersky Security Center.
- Zadejte heslo tokenu nebo čipové karty připojené k počítači.

Použití tokenu nebo čipové karty bude k dispozici, pouze pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES256. Pokud byly pevné disky počítače zašifrovány pomocí šifrovacího algoritmu AES56, přiřazení souboru elektronického certifikátu k příkazu bude zamítnuto.

BitLocker Drive Encryption

BitLocker je šifrovací technologie zabudovaná do operačních systémů Windows. Aplikace Kaspersky Endpoint Security vám umožňuje řídit a spravovat technologii Bitlocker pomocí aplikace Kaspersky Security Center. BitLocker šifruje logické svazky. BitLocker nelze použít pro šifrování vyměnitelných jednotek. Podrobnosti o technologii BitLocker najdete v dokumentaci společnosti Microsoft.

BitLocker poskytuje zabezpečené úložiště přístupových klíčů pomocí modulu TPM (Trusted Platform Module). *Trusted Platform Module (TPM)* je mikročip vyvinutý pro poskytování základních funkcí souvisejících se zabezpečením (například k ukládání šifrovacích klíčů). Modul TPM je obvykle nainstalován na základní desce počítače a komunikuje se všemi ostatními součástmi systému prostřednictvím hardwarové sběrnice. Použití modulu TPM je nejbezpečnějším způsobem uložení přístupových klíčů nástroje BitLocker, protože modul poskytuje ověření integrity systému před spuštěním. Jednotky v počítači můžete šifrovat i bez modulu TPM. V tomto případě bude přístupový klíč zašifrován pomocí hesla. BitLocker používá následující metody ověřování:

- TPM.
- TPM a PIN.
- Heslo.

Po zašifrování jednotky vytvoří nástroj BitLocker hlavní klíč. Aplikace Kaspersky Endpoint Security odešle hlavní klíč do aplikace Kaspersky Security Center, abyste mohli obnovit přístup na disk, například pokud uživatel zapomene heslo.

Pokud uživatel zašifruje disk pomocí nástroje BitLocker, Kaspersky Endpoint Security pošle informace o šifrování disku do aplikace Kaspersky Security Center. Kaspersky Endpoint Security nicméně do aplikace Kaspersky Security Center neposílá hlavní klíč, takže nebude možné obnovit přístup na disk pomocí aplikace Kaspersky Security Center. Aby nástroj BitLocker správně fungoval s aplikací Kaspersky Security Center, dešifrujte jednotku a znovu ji zašifrujte pomocí zásady. Jednotku můžete dešifrovat místně nebo pomocí zásady.

Po zašifrování systémového pevného disku musí uživatel před spuštěním operačního systému projít ověřením nástrojem BitLocker. Po ověření umožní nástroj BitLocker uživatelům přihlášení. BitLocker nepodporuje technologii jednotného přihlašování (SSO).

Pokud používáte zásady skupiny systému Windows, vypněte správu nástroje BitLocker v nastavení zásad. Nastavení zásad systému Windows může být v rozporu s nastavením zásad aplikace Kaspersky Endpoint Security. Při šifrování jednotky mohou nastat chyby.

Nastavení součásti Kaspersky Disk Encryption

Parametr	Popis
Režim šifrování	**Šifrovat všechny pevné disky**. Je-li vybrána tato položka, aplikace zašifruje všechny pevné disky, když jsou použity zásady. Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém je nainstalována příslušná aplikace. **Dešifrovat všechny pevné disky**. Je-li vybrána tato položka, aplikace dešifruje všechny pevné disky, když jsou použity zásady. **Ponechat bez změny**. Je-li vybrána tato položka, aplikace ponechá disky v předchozím stavu, když jsou použity zásady. Pokud byl disk zašifrován, zůstane zašifrovaný. Pokud byl disk dešifrovaný, zůstane dešifrovaný. Tato položka je ve výchozím nastavení vybrána.
Při šifrování	Je-li toto políčko zaškrtnuto, aplikace vytváří účty agenta ověřování na základě seznamu

automaticky vytvářet pro uživatele systému Windows účty ověřovacího agenta	uživatelských účtů Windows v počítači. Ve výchozím nastavení aplikace Kaspersky Endpoint Security používá všechny místní a doménové účty, pomocí kterých se uživatel přihlásil k operačnímu systému za posledních 30 dní.
Nastavení vytváření účtů ověřovacího agenta	**Všechny účty v počítači**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku účty ověřovacího agenta pro všechny počítačové účty, které kdy byly aktivní. **Všechny účty domén v počítači**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku účty ověřovacího agenta pro všechny počítačové účty patřící do určité domény, které kdy byly aktivní. **Všechny místní účty v počítači**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku účty ověřovacího agenta pro všechny místní počítačové účty, které kdy byly aktivní. **Místní správce**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku účet místního správce. **Správce počítače**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku účet ověřovacího agenta pro účet, jehož vlastnosti ve službě Active Directory značí, že se jedná o účet pro správu. **Aktivní účet**. Pokud je toto políčko zaškrtnuto, vytvoří aplikace Kaspersky Endpoint Security při spuštění úlohy úplného šifrování disku automaticky účet ověřovacího agenta pro počítačový účet, který je během úlohy aktivní.
Vytvářet pro všechny uživatele tohoto počítače účty ověřovacího agenta automaticky při přihlášení	Je-li toto políčko zaškrtnuto, aplikace před spuštěním ověřovacího agenta zkontroluje informace o uživatelských účtech Windows v počítači. Pokud aplikace Kaspersky Endpoint Security zjistí uživatelský účet systému Windows, který nemá účet ověřovacího agenta, aplikace vytvoří nový účet pro přístup k šifrovaným jednotkám. Nový účet ověřovacího agenta bude mít následující výchozí nastavení: pouze přihlašování chráněné heslem a změna hesla při prvním ověřování. Proto u počítačů s již zašifrovanými jednotkami nemusíte ručně přidávat účty agenta ověřování pomocí úlohy *Správa účtů ověřovacího agenta*.
Uložit uživatelské jméno zadané v ověřovacím agentovi	Pokud je toto políčko zaškrtnuto, aplikace uloží název účtu ověřovacího agenta. Název účtu bude nutné zadat při příštím pokusu o dokončení autorizace v ověřovacím agentovi pod stejným účtem.
Zašifrovat pouze využité místo na disku	Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat funkci, která omezuje oblast šifrování pouze na využité sektory pevného disku. Díky tomuto omezení lze zkrátit dobu šifrování. Povolení nebo zakázání funkce **Zašifrovat pouze využité místo na disku (zkracuje dobu šifrování)** po spuštění šifrování nezmění toto nastavení, dokud nebudou pevné disky zašifrované. Před zahájením šifrování je třeba políčko zaškrtnout nebo zrušit jeho zaškrtnutí. Pokud je toto políčko zaškrtnuto, budou šifrovány pouze části pevného disku, na kterých jsou soubory. Aplikace Kaspersky Endpoint Security automaticky šifruje nová data při jejich přidání.

	Jestliže je zaškrtnutí tohoto políčka zrušeno, bude šifrováno celý pevný disk, včetně zbytkových fragmentů dříve odstraněných a upravených souborů. Tuto funkci doporučujeme používat u nových disků, jejichž data ještě nebyla upravena nebo odstraněna. Pokud použijete šifrování u pevného disku, který se již používá, doporučujeme šifrovat celý pevný disk. Zajistíte tím ochranu všech dat, a to i odstraněných dat, která se dají případně obnovit. Toto políčko není ve výchozím nastavení zaškrtnuto.
Použít funkci Legacy USB Support	Toto zaškrtávací políčko povoluje / zakazuje funkci Legacy USB Support. *Legacy USB Support* **je** funkce BIOS/UEFI, která vám umožní používat zařízení USB (například token zabezpečení) během fáze spouštění počítače před spuštěním operačního systému (režim BIOS). Funkce Legacy USB Support neovlivňuje podporu zařízení USB po spuštění operačního systému. Pokud je toto políčko zaškrtnuto, bude podpora zařízení USB při počátečním spouštění počítače povolena. Je-li funkce Legacy USB Support aktivována, ověřovací agent v režimu BIOS nepodporuje práci s tokeny přes USB. Tuto funkci doporučujeme používat pouze v případě, že dochází k problémům s kompatibilitou hardwaru, a pouze u počítačů, ve kterých k problémům dochází.
Nastavení hesla	Nastavení síly hesla účtu ověřovacího agenta. Můžete také povolit nebo zakázat používání technologie SSO (Single Sign-On). Technologie SSO umožňuje používat stejné přihlašovací údaje pro přístup k šifrovaným pevným diskům i k přihlášení k operačnímu systému. Pokud je toto políčko zaškrtnuto, musíte při přístupu k šifrovaným pevným diskům a následnému automatickému přihlášení k operačnímu systému zadat přihlašovací údaje k účtu. Jestliže je zaškrtnutí tohoto políčka zrušeno, je nutné při přístupu k šifrovaným pevným jednotkám a následnému přihlášení k operačnímu systému zadat zvlášť přihlašovací údaje pro přístup k šifrovaným pevným jednotkám i přihlašovací údaje k uživatelskému účtu operačního systému.
Texty nápovědy	**Ověření**. Text nápovědy, který se objeví v okně Ověřovací agent při zadávání přihlašovacích údajů k účtu. **Změnit heslo**. Text nápovědy, který se objeví v okně Ověřovací agent při změně hesla pro účet tohoto agenta. **Obnovit heslo**. Text nápovědy, který se objeví v okně Ověřovací agent při obnovení hesla pro účet tohoto agenta.

Nastavení součásti BitLocker Drive Encryption

Parametr	Popis
Režim šifrování	**Šifrovat všechny pevné disky**. Je-li vybrána tato položka, aplikace zašifruje všechny pevné disky, když jsou použity zásady. Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém je nainstalována příslušná aplikace.

	Dešifrovat všechny pevné disky. Je-li vybrána tato položka, aplikace dešifruje všechny pevné disky, když jsou použity zásady. **Ponechat bez změny**. Je-li vybrána tato položka, aplikace ponechá disky v předchozím stavu, když jsou použity zásady. Pokud byl disk zašifrován, zůstane zašifrovaný. Pokud byl disk dešifrovaný, zůstane dešifrovaný. Tato položka je ve výchozím nastavení vybrána.
Povolit použití ověřování BitLocker vyžadující vstup z klávesnice před spuštěním na tabletech	Tímto zaškrtávacím políčkem lze povolit nebo zakázat použití ověřování vyžadujícího zadání dat v prostředí před spuštěním, i když platforma nemá možnost vstupu před spuštěním (například s dotykovými klávesnicemi na tabletech). V prostředí před spuštěním není k dispozici dotyková obrazovka tabletů. Aby bylo možné v tabletech dokončit ověřování pomocí technologie BitLocker, uživatel musí připojit například klávesnici USB. Je-li toto políčko zaškrtnuto, použití ověřování vyžadujícího vstup před spuštěním bude povoleno. Toto nastavení doporučujeme použít pouze pro zařízení, která mají alternativní nástroje pro zadání dat v prostředí před spuštěním, jako je například USB klávesnice kromě dotykové klávesnice. Není-li toto políčko zaškrtnuto, technologii BitLocker Drive Encryption nelze používat na tabletech.
Použít hardwarové šifrování	Pokud je políčko zaškrtnuté, aplikace použije hardwarové šifrování. Tím se zvyšuje rychlost šifrování a bude využito méně výpočetních prostředků.
Zašifrovat pouze využité místo na disku (Windows 8 a novější verze)	Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat funkci, která omezuje oblast šifrování pouze na využité sektory pevného disku. Díky tomuto omezení lze zkrátit dobu šifrování. Povolení nebo zakázání funkce **Zašifrovat pouze využité místo na disku (zkracuje dobu šifrování)** po spuštění šifrování nezmění toto nastavení, dokud nebudou pevné disky zašifrované. Před zahájením šifrování je třeba políčko zaškrtnout nebo zrušit jeho zaškrtnutí. Pokud je toto políčko zaškrtnuto, budou šifrovány pouze části pevného disku, na kterých jsou soubory. Aplikace Kaspersky Endpoint Security automaticky šifruje nová data při jejich přidání. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude šifrováno celý pevný disk, včetně zbytkových fragmentů dříve odstraněných a upravených souborů. Tuto funkci doporučujeme používat u nových disků, jejichž data ještě nebyla upravena nebo odstraněna. Pokud použijete šifrování u pevného disku, který se již používá, doporučujeme šifrovat celý pevný disk. Zajistíte tím ochranu všech dat, a to i odstraněných dat, která se dají případně obnovit. Toto políčko není ve výchozím nastavení zaškrtnuto.
Nastavení ověřování	**Použít heslo (Windows 8 a novější verze)** Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security vyzve uživatele k zadání hesla, když se uživatel pokusí o přístup k šifrovanému disku. Tuto možnost lze vybrat, když není čip TPM (Trusted Platform Module) použit.

Použít čip TPM (Trusted Platform Module)

Je-li tato možnost vybrána, technologie BitLocker použije čip TPM (Trusted Platform Module).

Trusted Platform Module (TPM) je mikročip vyvinutý pro poskytování základních funkcí souvisejících se zabezpečením (například k ukládání šifrovacích klíčů). Čip TPM je obvykle instalovaný na základní desce počítače a komunikuje se všemi ostatními součástmi systému prostřednictvím hardwarového rozhraní.

U počítačů se systémem Windows 7 nebo Windows Server 2008 R2 je k dispozici pouze šifrování pomocí modulu TPM. Pokud modul TPM není nainstalován, šifrování nástroje BitLocker není možné. Použití hesla v těchto počítačích není podporováno.

Zařízení vybavené čipem TPM (Trusted Platform Module) může vytvořit šifrovací klíče, které lze dešifrovat pouze pomocí tohoto zařízení. Čip TPM (Trusted Platform Module) šifruje šifrovací klíče pomocí vlastního kořenového klíče úložiště. Kořenový klíč úložiště je uložen v čipu TPM (Trusted Platform Module). Ten poskytuje další úroveň ochrany před pokusy o hacknutí šifrovacích klíčů.

Tato akce je nastavena jako výchozí.

Pro přístup k šifrovacímu klíči můžete nastavit další vrstvu ochranu a klíč zašifrovat heslem nebo kódem PIN:

- **Použít kód PIN z TPM**. Je-li toto políčko zaškrtnuto, uživatel může použít kód PIN k získání přístupu k šifrovacímu klíči, který je uložen v čipu TPM (Trusted Platform Module).
  Pokud není toto zaškrtávací políčko zaškrtnuto, uživatelé nebudou moci používat kódy PIN. Pro přístup k šifrovacímu klíči musí uživatel zadat heslo.
  Uživateli můžete povolit používání rozšířeného kódu PIN. *Rozšířený PIN* umožňuje kromě numerických znaků používat i další znaky: velká a malá písmena latinky, speciální znaky a mezery.

- **Použít TPM (Trusted Platform Module); pokud není k dispozici, použít heslo**. Pokud není toto políčko zaškrtnuto, uživatel může získat přístup k šifrovacím klíčům pomocí hesla, když není čip TPM (Trusted Platform Module) k dispozici.

  Pokud políčko není zaškrtnuto a TPM není k dispozici, úplné šifrování disku se nespustí.

Šifrování na úrovni souborů

Můžete zkompilovat seznamy souborů podle přípony nebo skupiny přípon a seznamy složek uložených na místních počítačových discích a vytvořit pravidla šifrování souborů vytvořených určitými aplikacemi. Po použití zásad aplikace Kaspersky Security Center zašifruje a dešifruje následující soubory:

- Soubory jednotlivě přidané na seznamy pro šifrování a dešifrování.
- Soubory uložené ve složkách přidaných na seznamy pro šifrování a dešifrování.
- Soubory vytvořené samostatnými aplikacemi.

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Šifrování souborů má následující zvláštní funkce:

- Aplikace Kaspersky Endpoint Security šifruje/dešifruje soubory v předdefinovaných složkách jen pro místní uživatelské profily v operačním systému. Aplikace Kaspersky Endpoint Security nešifruje ani nedešifruje soubory v předdefinovaných složkách uživatelských profilů roamingu, povinných uživatelských profilů, dočasných uživatelských profilů ani soubory v přesměrovaných složkách.

- Aplikace Kaspersky Endpoint Security nešifruje soubory, jejichž změnou by mohlo dojít k poškození operačního systému a nainstalovaných aplikací. Na seznamu položek vyloučených ze šifrování jsou například následující soubory a složky se všemi vnořenými složkami:

  - %WINDIR%;
  - %PROGRAMFILES% a %PROGRAMFILES(X86)%;
  - Soubory registru systému Windows.

  Seznam položek vyloučených ze šifrování nelze zobrazit ani upravit. I když lze soubory a složky, které jsou na seznamu položek vyloučených ze šifrování, přidat na seznam šifrovaných položek, během šifrování souborů se nezašifrují.

Nastavení součásti Šifrování na úrovni souborů

Parametr	Popis
Správa šifrování	**Ponechat bez změny**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security ponechá soubory a složky beze změny, aniž by je zašifrovala nebo dešifrovala. **Šifrovat podle pravidel**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security šifruje soubory a složky podle pravidel šifrování, dešifruje soubory a složky podle pravidel dešifrování a reguluje přístup aplikací k šifrovaným souborům podle pravidel aplikace. **Dešifrovat vše**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security dešifruje všechny šifrované soubory a složky.
Pravidla šifrování	Na této kartě jsou zobrazena pravidla šifrování souborů uložených na místních discích. Soubory můžete přidat následujícím způsobem: • **Předdefinované složky**. Aplikace Kaspersky Endpoint Security umožňuje přidat následující oblasti: **Dokumenty**. Soubory ve standardní systémové složce *Dokumenty* a jejích podsložkách. **Oblíbené položky**. Soubory ve standardní systémové složce *Oblíbené položky* a jejích podsložkách. **Plocha**. Soubory ve standardní systémové složce *Plocha* a jejích podsložkách. **Dočasné soubory**. Dočasné soubory související s provozováním aplikací nainstalovaných v počítači. Například aplikace sady Microsoft Office vytvářejí dočasné soubory obsahující záložní kopie dokumentů. **Soubory aplikace Outlook**. Soubory související s provozem poštovního klienta aplikace Outlook: datové soubory (PST), offline datové soubory (OST), offline soubory adresáře (OAB) a soubory osobních adresářů (PAB). • **Složky**. Cestu ke složce můžete napsat ručně. Při přidávání cesty ke složce dodržujte následující pravidla: Použijte proměnnou prostředí (například `%FOLDER%\UserFolder\`). Proměnnou prostředí můžete použít pouze jednou a pouze na začátku cesty.

	Nepoužívejte relativní cesty. Můžete použít sadu `\..\` (např. `C:\Users\..\UserFolder\`). Sada `\..\` označuje přechod do nadřazené složky. Nepoužívejte znaky `*` ani `?`. Nepoužívejte cesty UNC. Jako oddělovač znaků použijte `;` nebo `,`. • **Soubory podle přípony**. Ze seznamu můžete vybrat skupiny přípon, například skupinu rozšíření *Archivy*. Příponu souboru můžete také přidat ručně.
Pravidla dešifrování	Na této kartě jsou zobrazena pravidla dešifrování souborů uložených na místních discích.
Pravidla pro aplikace	Na kartě se zobrazuje tabulka, která obsahuje pravidla přístupu k šifrovaným souborům pro aplikace a pravidla šifrování pro soubory, které byly vytvořeny nebo upraveny jednotlivými aplikacemi.
Nastavení hesla pro šifrované balíčky	Při vytváření šifrovaných balíčků je třeba splnit požadavky na sílu hesla.

Šifrování vyměnitelných jednotek

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery.

Aplikace Kaspersky Endpoint Security podporuje šifrování souborů v souborových systémech FAT32 a NTFS. Pokud je k počítači připojena vyměnitelná jednotka s nepodporovaným souborovým systémem, úloha šifrování pro tuto vyměnitelnou jednotku skončí chybou a aplikace Kaspersky Endpoint Security přiřadí vyměnitelné jednotce stav jen pro čtení.

Chcete-li chránit data na vyměnitelných jednotkách, můžete použít následující typy šifrování:

- Úplné šifrování disku (FDE).

  Šifrování celé vyměnitelné jednotky, včetně systému souborů.

  Není možné přistupovat k šifrovaným datům mimo podnikovou síť. Je také nemožné přistupovat k šifrovaným datům v podnikové síti, pokud počítač není připojen k aplikaci Kaspersky Security Center (např. na hostovaném počítači).

- Šifrování na úrovni souborů (FLE).

  Šifrování pouze souborů na vyměnitelné jednotce. Systém souborů zůstává nezměněn.

  Šifrování souborů na vyměnitelných jednotkách umožňuje získat přístup k datům mimo podnikovou síť pomocí zvláštního režimu s názvem *přenosný režim*.

Během šifrování vytvoří aplikace Kaspersky Endpoint Security hlavní klíč. Aplikace Kaspersky Endpoint Security ukládá hlavní klíč do následujících úložišť:

- Kaspersky Security Center.
- Počítač uživatele.

  Hlavní klíč je šifrován tajným klíčem uživatele.
- Vyměnitelná jednotka.

  Hlavní klíč je šifrován veřejným klíčem aplikace Kaspersky Security Center.

Po dokončení šifrování jsou data na vyměnitelné jednotce přístupná v podnikové síti, jako kdyby byla na běžné nešifrované vyměnitelné jednotce.

Přístup k šifrovaným datům

Po připojení vyměnitelné jednotky se šifrovanými daty provádí aplikace Kaspersky Endpoint Security následující akce:

1. Vyhledá hlavní klíč v místním úložišti v počítači uživatele.

   Pokud je nalezen hlavní klíč, získá uživatel přístup k datům na vyměnitelné jednotce.

   Pokud hlavní klíč není nalezen, provede Kaspersky Endpoint Security následující akce:

   a. Odešle žádost do aplikace Kaspersky Security Center.

      Po přijetí žádosti aplikace Kaspersky Security Center odešle odpověď, která obsahuje hlavní klíč.

   b. Aplikace Kaspersky Endpoint Security uloží hlavní klíč do místního úložiště v počítači uživatele pro následné operace se šifrovanou vyměnitelnou jednotkou.
2. Dešifruje data.

Zvláštní funkce šifrování vyměnitelné jednotky

Šifrování vyměnitelných jednotek má následující speciální funkce:

- Zásady s nastavením předvoleb pro šifrování vyměnitelných jednotek se vytváří pro určitou skupinu spravovaných počítačů. Proto je výsledek použití zásady aplikace Kaspersky Security Center nakonfigurované pro šifrování/dešifrování vyměnitelných jednotek závislý na počítači, ke kterému je vyměnitelná jednotka připojená.
- Aplikace Kaspersky Endpoint Security nešifruje ani nedešifruje soubory, které jsou na vyměnitelných jednotkách ve stavu jen pro čtení.
- Následující typy zařízení jsou podporována jako vyměnitelné jednotky:
  - datová média připojená přes sběrnici USB;
  - pevné disky připojené přes sběrnice USB a FireWire;
  - jednotky SSD připojené přes sběrnice USB a FireWire.

Nastavení součásti Šifrování vyměnitelných jednotek

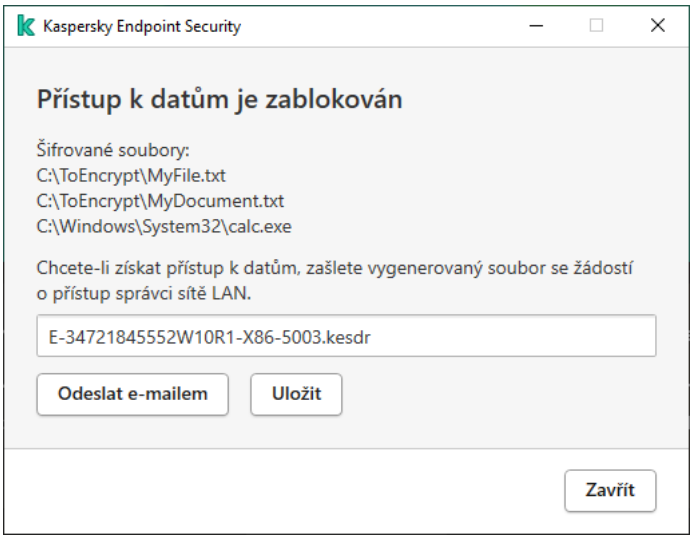
Parametr	Popis
Správa šifrování	**Šifrovat celou vyměnitelnou jednotku**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při použití zásad se zadanými nastaveními šifrování pro vyměnitelné jednotky zašifruje vyměnitelné jednotky po jednotlivých oddílech, včetně souborových systémů. **Šifrovat všechny soubory**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při použití zásad se zadanými nastaveními šifrování pro vyměnitelné jednotky zašifruje všechny soubory, které jsou uloženy na vyměnitelných jednotkách. Aplikace Kaspersky Endpoint Security již zašifrované soubory znovu nešifruje. Obsah souborového systému vyměnitelné jednotky, včetně struktury složek a názvů zašifrovaných souborů, není zašifrován a zůstane přístupný. **Šifrovat pouze nové soubory**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při použití zásad se zadanými nastaveními šifrování pro vyměnitelné jednotky zašifruje pouze soubory, které byly přidány nebo upraveny na vyměnitelných jednotkách po posledním použití zásad Kaspersky Security Center. Tento režim šifrování je praktický, když je vyměnitelná jednotka použita pro osobní i pracovní účely. Tento režim šifrování umožňuje ponechat všechny staré soubory beze změny a zašifrovat pouze soubory, které uživatel vytvoří na pracovním počítači s nainstalovanou aplikací Kaspersky Endpoint Security a povolenou funkcí šifrování. V důsledku toho bude přístup k osobním souborům vždy k dispozici, bez ohledu na to, zda je v počítači s povolenou funkcí šifrování nainstalována aplikace Kaspersky Endpoint Security či nikoli. **Dešifrovat celou vyměnitelnou jednotku**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při použití zásad se zadanými nastaveními šifrování pro vyměnitelné jednotky dešifruje všechny zašifrované soubory, které jsou uloženy na vyměnitelných jednotkách, a také souborové systémy vyměnitelných jednotek, pokud byly dříve zašifrovány. **Ponechat bez změny**. Je-li vybrána tato položka, aplikace ponechá disky v předchozím stavu, když jsou použity zásady. Pokud byl disk zašifrován, zůstane zašifrovaný. Pokud byl disk dešifrovaný, zůstane dešifrovaný. Tato položka je ve výchozím nastavení vybrána.
Mobilní režim	Tímto zaškrtávacím políčkem lze povolit nebo zakázat přípravu vyměnitelné jednotky, díky které lze přistupovat k souborům uloženým na vyměnitelné jednotce v počítačích mimo podnikovou síť. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security vyzve uživatele k zadání hesla před zašifrováním souborů na vyměnitelné jednotce při použití zásad. Heslo je nutné k přístupu k souborům zašifrovaným na vyměnitelné jednotce v počítačích mimo podnikovou síť. Můžete nakonfigurovat sílu hesla. Mobilní režim je k dispozici pro režimy **Šifrovat všechny soubory** nebo **Šifrovat pouze nové soubory**.
Zašifrovat pouze využité místo na disku	Tímto zaškrtávacím políčkem lze povolit nebo zakázat režim šifrování, ve kterém budou zašifrovány pouze využité oddíly disku. Tento režim je doporučen pro nové disky, jejichž data ještě nebyla upravena nebo odstraněna. Je-li políčko zaškrtnuto, budou zašifrovány pouze části disku, na kterých jsou soubory. Aplikace Kaspersky Endpoint Security automaticky šifruje nová data při jejich přidání. Není-li políčko zaškrtnuto, bude zašifrován celý disk, včetně zbytkových fragmentů dříve odstraněných a upravených souborů. Funkce pro šifrování pouze obsazeného místa je k dispozici pouze pro režim **Šifrovat celou vyměnitelnou jednotku**. Po spuštění šifrování se povolením nebo zakázáním funkce **Zašifrovat pouze využité místo na disku** toto nastavení nezmění. Před zahájením šifrování je třeba políčko zaškrtnout nebo zrušit jeho zaškrtnutí.

Pravidla šifrování pro vybraná zařízení	Tato tabulka obsahuje zařízení, pro která jsou definována vlastní pravidla šifrování. Pravidla šifrování pro jednotlivé vyměnitelné jednotky můžete vytvořit následujícími způsoby:
	• Přidejte vyměnitelnou jednotku ze seznamu důvěryhodných zařízení pro součást Kontrola zařízení.
	• Ruční přidání vyměnitelné jednotky:
	  • ID zařízení (ID hardwaru neboli HWID)
	  • Podle modelu zařízení: ID dodavatele (VID) a ID produktu (PID)

Povolit šifrování vyměnitelné jednotky v režimu offline	Pokud je toto políčko zaškrtnuto, bude aplikace Kaspersky Endpoint Security vyměnitelné jednotky šifrovat i v případě, že není navázáno připojení k aplikaci Kaspersky Security Center. V takovém případě jsou data vyžadující dešifrování vyměnitelných jednotek uložena na pevném disku počítače, ke kterému je vyměnitelná jednotka připojena, a nejsou přenášena do aplikaci Kaspersky Security Center. Není-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezašifruje vyměnitelné jednotky bez připojení ke službě Kaspersky Security Center.
Nastavení hesla přenosného režimu	Nastavení síly hesla pro Mobilního správce souborů.

Šablony (šifrování dat)

Po šifrování dat může aplikace Kaspersky Endpoint Security omezit přístup k datům, například z důvodu změny infrastruktury organizace a změny na serveru správy aplikace Kaspersky Security Center. Pokud uživatel nemá přístup k šifrovaným datům, může požádat správce o přístup. Jinými slovy musí uživatel poslat správci přístupový soubor žádosti. Uživatel potom musí nahrát soubor odpovědi obdržený od správce do aplikace Kaspersky Endpoint Security. Aplikace Kaspersky Endpoint Security vám umožňuje vyžádat si přístup k datům od správce prostřednictvím e-mailu (viz obrázek níže).



Žádost o přístup k šifrovaným datům

K dispozici je šablona pro hlášení nedostatku přístupu k šifrovaným datům. Pro pohodlí uživatele můžete vyplnit následující pole:

- **Komu**. Zadejte e-mailovou adresu skupiny správce s právy na funkce šifrování dat.
- **Předmět**. Zadejte předmět e-mailu s žádostí o přístup k šifrovaným souborům. Můžete například přidat k filtrovaným zprávám přidat štítky.
- **Zpráva**. V případě potřeby změňte obsah zprávy. Proměnné můžete použít k získání potřebných dat (například proměnná `%USER_NAME%`).

Výjimky

Důvěryhodná zóna je správcem konfigurovaný seznam objektů a aplikací, které aplikace Kaspersky Endpoint Security nesleduje, když jsou aktivní.

Správce vytvoří důvěryhodnou zónou nezávisle a bere v potaz funkce objektů, které jsou zpracovávány, a aplikací nainstalovaných v počítači. Zahrnutí objektů a aplikací do důvěryhodné zóny může být vyžadováno v případech, kdy aplikace Kaspersky Endpoint Security zablokuje přístup k určitému objektu nebo aplikaci, ale vy jste si jisti, že daný objekt nebo aplikace jsou neškodné. Správce může také uživateli umožnit vytvoření vlastní místní důvěryhodné zóny pro konkrétní počítač. Tímto způsobem mohou uživatelé kromě obecné důvěryhodné zóny v zásadách vytvářet také vlastní místní seznamy výjimek a důvěryhodných aplikací.

Výjimky z kontroly

Výjimka z kontroly je sada podmínek, které je nutné splnit, aby aplikace Kaspersky Endpoint Security nekontrolovala určitý objekt na přítomnost virů nebo jiných hrozeb.

Výjimky z kontroly umožňují bezpečně používat legitimní software, který může být pachateli využit k poškození počítače nebo data uživatele. I když tyto aplikace nemají žádnou škodlivou funkci, mohou být zneužity útočníky. Podrobnosti o legitimním softwaru, který může být využíván pachateli k poškození počítače nebo osobních údajů uživatele, najdete na webových stránkách encyklopedie IT Kaspersky.

Tyto aplikace mohou být aplikací Kaspersky Endpoint Security zablokovány. Pokud tyto aplikace blokovat nechcete, můžete pro ně nakonfigurovat výjimky z kontroly. To lze provést tak, že přidáte název nebo masku názvu uvedené v encyklopedii IT Kaspersky do důvěryhodné zóny. Například často používáte aplikaci Radmin ke vzdálené správě počítačů. Aplikace Kaspersky Endpoint Security vyhodnocuje tuto činnost jako podezřelou a může ji zablokovat. Aby tato aplikace nemohla být zablokována, vytvořte výjimku z kontroly za použití názvu nebo masky názvu, které jsou uvedené v encyklopedii IT Kaspersky.

Je-li ve vašem počítači nainstalována aplikace shromažďující a odesílající informace ke zpracování, aplikace Kaspersky Endpoint Security může tuto aplikaci klasifikovat jako malware. Aby k tomu nedošlo, můžete tuto aplikaci vyloučit z kontroly nakonfigurováním aplikace Kaspersky Total Security podle postupu uvedeného v tomto dokumentu.

Výjimky z kontroly mohou být použity následujícími součástmi a úlohami aplikace, které jsou nakonfigurovány správcem systému:

- Detekce chování.
- Prevence zneužití.
- Prevence narušení hostitele.

- Ochrana před souborovými hrozbami.
- Ochrana před webovými hrozbami.
- Ochrana před hrozbami v poště.
- Úlohy kontroly.

Seznam důvěryhodných aplikací

Seznam důvěryhodných aplikací je seznam aplikací, jejichž činnost se soubory a v síti (včetně škodlivé činnost) a přístup k systémovému registru nejsou aplikací Kaspersky Endpoint Security sledovány. Aplikace Kaspersky Endpoint Security ve výchozím nastavení kontroluje objekty, které jsou otevírané, spouštěné nebo ukládané jakýmkoli procesem aplikace, a kontroluje činnost všech aplikací a veškerý síťový provoz, který tyto aplikace vygenerují. Aplikace, která byla přidána do seznamu důvěryhodných aplikací, je však z kontroly aplikací Kaspersky Endpoint Security vyloučena.

Pokud například považujete objekty používané standardní aplikací Poznámkový blok v systému Microsoft Windows za bezpečnou, takže ji není třeba kontrolovat (tj. této aplikaci důvěřujete), může ji přidat na seznam důvěryhodných aplikací. Při kontrole jsou pak vynechány objekty, které tato aplikace používá.

Kromě toho mohou být některé akce, které jsou klasifikované aplikací Kaspersky Endpoint Security jako podezřelé, v kontextu funkcí řady aplikací bezpečné. Například zachycení textu psaného na klávesnici je běžný proces pro automatické přepínače rozvržení klávesnice (například Punto Switcher). Pokud chcete zohlednit specifika takových aplikací a vyloučit jejich činnost ze sledování, doporučujeme je přidat na seznam důvěryhodných aplikací.

Vyloučení důvěryhodných aplikací z kontrol umožňuje zabránit konfliktům kompatibility mezi aplikací Kaspersky Endpoint Security a jinými programy (například problém zdvojené kontroly síťového provozu počítače třetí strany pomocí aplikace Kaspersky Endpoint Security a jiné antivirové aplikace) a také zvyšuje výkon počítače, což je důležité při použití serverových aplikací.

U důvěryhodných aplikací jsou i nadále příslušné spustitelné soubory a procesy kontrolovány na viry či jiný malware. Za použití výjimek z kontroly lze aplikaci plně vyloučit z kontrol prováděných aplikací Kaspersky Endpoint Security.

Nastavení výjimek

Parametr	Popis
Typy zjištěných objektů	Bez ohledu na nakonfigurovaná nastavení, aplikace Kaspersky Endpoint Security vždy detekuje a blokuje viry, červy a trojské koně. Mohou způsobit závažné poškození počítače. • Viry a červy

Podkategorie: viry a červy (Viruses_and_Worms)

Úroveň hrozby: vysoká

Klasické viry a červy provádějí akce, které nejsou uživatelem schváleny. Mohou vytvářet kopie samy sebe, které se mohou replikovat.

Klasický virus

Když klasický virus pronikne do počítače, infikuje soubor, aktivuje se, provede škodlivé akce a přidá kopie sebe sama do jiných souborů.

Klasický virus se násobí pouze v místních prostředcích počítače, sám o sobě nemůže proniknout do jiných počítačů. Do jiného počítače může být přenesen, pouze pokud přidá kopii sebe sama do souboru, který je uložen ve sdílené složce nebo na vloženém disku CD, nebo pokud uživatel přepošle e-mailovou zprávu s připojeným infikovaným souborem.

Kód klasického viru může proniknout do různých oblastí počítačem operačních systémů a aplikací. V závislosti na prostředí se viry dělí na *souborové viry*, *spouštěcí viry*, *skriptové viry* a *makro viry*.

Viry mohou infikovat soubory různými technikami. *Přepisovací* viry přepíší svůj kód přes kód infikovaného souboru, čímž se obsah souboru vymaže. Infikovaný soubor přestane fungovat a nebude možné jej obnovit. *Parazitické* viry upravují soubory a zanechají se plně nebo částečně funkční. *Doprovodné viry* neupravují soubory, ale vytvářejí duplicitní soubory. Při otevření infikovaného souboru se spustí jeho duplikát (který je ve skutečnosti virem). Setkat se můžete také s následujícími typy virů: *odkazové viry*, *viry OBJ*, *viry LIB*, viry *zdrojového kódu* a mnoho dalších.

Červy

Stejně jako u klasického viru se po proniknutí do počítače aktivuje kód červa a provede škodlivé akce. Červy své označení získaly díky své schopnosti „plazit“ se z jednoho počítače do druhého a šířit kopie prostřednictvím různých datových kanálů bez povolení uživatele.

Hlavním prvkem, který umožňuje rozlišovat mezi různými typy červů, je způsob jejich šíření. Následující tabulka poskytuje přehled různých typů červů, které jsou klasifikovány dle způsobu šíření.

Způsob šíření červů

Typ	Název	Popis
Email-Worm	Email-Worm	Šíří se e-mailem. Infikovaná e-mailová zpráva obsahuje připojený soubor s kopií červa nebo odkaz na soubor nahraný na webovou stránku, která mohla být hacknuta nebo vytvořena speciálně pro tento účel. Když připojený soubor otevřete, červ se aktivuje. Když kliknete na odkaz, stáhnete a poté otevřete soubor, červ začne provádět škodlivé akce. Poté začne šířit své kopie, vyhledávat další e-mailové adresy a odesílat na ně infikované zprávy.

Červ IM	Klienti IM	Šíří se prostřednictvím klientů IM. Takové červy obvykle odesílají zprávy, které obsahují odkaz na soubor s kopií červa na webu, s využitím seznamů kontaktů uživatele. Když uživatel stáhne a otevře soubor, červ se aktivuje.
Červ IRC	Červi internetových konverzací	Šíří se prostřednictvím IRC (Internet Relay Chats), což jsou systémy služeb, které umožňují komunikaci s dalšími lidmi přes internet v reálném čase. Tyto červy zveřejní soubor s kopií jich samých nebo odkazem na soubor v internetové konverzaci. Když uživatel stáhne a otevře soubor, červ se aktivuje.
Síťový červ	Síťové červy	Tyto červy se šíří počítačovými sítěmi. Na rozdíl od jiných typů červů se běžný síťový červ šíří bez účasti uživatele. V místní síti hledá počítače, které obsahují zranitelné programy. Za tímto účelem odesílá speciálně vytvořený síťový paket (exploit), který obsahuje kód červa nebo jeho část. Pokud je v síti zranitelný počítač, obdrží takový síťový paket. Když červ zcela pronikne do počítače, aktivuje se.
Červ P2P	Síťové červy pro sdílení souborů	Šíří se přes sítě P2P pro sdílení souborů. Aby mohl červ infiltrovat síť P2P, zkopíruje se do složky pro sdílení souboru, která se obvykle nachází v počítači uživatele. V síti P2P se zobrazí informace o tomto souboru, aby uživatel mohl „najít“ infikovaný soubor v síti jako jakýkoli jiný soubor, stáhnout jej a otevřít. Propracovanější červy emulují síťový protokol určité sítě P2P: zobrazí kladné reakce na dotazy hledání a nabídnou kopie sebe sama ke stažení.
Červy	Další typy červů	Mezi další typy červů patří: • Červy, které šíří kopie sebe samých přes síťové prostředky. Pomocí funkcí operačního systémů prohledávají dostupné síťové složky, připojují se k počítačům na internetu a pokouší se získat plný přístup k diskovým jednotkám. Na rozdíl od dříve popsaných typů červů se jiné typy červů neaktivují samy, ale když uživatel otevře soubor, který obsahuje kopii červa. • Červi, kteří se šíří jinak než pomocí metod popsaných v předchozí tabulce (například červi šířící se mobilními telefony).

- Trojské koně

Podkategorie: Trojské koně

Úroveň hrozby: vysoká

Na rozdíl červů a virů se trojské koně samy nereplikují. Do počítače pronikají například přes e-mail nebo prohlížeč, když uživatel navštíví infikovanou webovou stránku. Trojské koně se spouští za účasti uživatele. Začínají provádět škodlivé akce ihned po spuštění.

Různé trojské koně se v infikovaných počítačích chovají různě. Mezi hlavní funkce trojských koňů patří blokování, úprava nebo ničení informací a zakázání počítačů nebo sítí. Trojské koně rovněž přijímají nebo odesílají soubory, spouští je, zobrazují zprávy na obrazovce, požadují webové stránky, stahují a instalují programy a restartují počítač.

Hackeři často používají sady trojských koňů.

Typy chování trojských koňů jsou popsány v následující tabulce.

Typy chování trojských koňů v infikovaném počítači

Typ	Název	Popis
Trojan-ArcBomb	Trojské koně – „archivní bomby“	Při rozbalení tyto archivy zvětší svou velikost do takové míry, že ovlivní činnost počítače. Když se uživatel pokusí takový archiv rozbalit, počítač se může zpomalit nebo zamrznout a pevný disk se může zaplnit „prázdnými“ daty. „Archivní bomby“ jsou nebezpečné především pro souborové a poštovní servery. Pokud server používá automatický systém zpracování příchozích informací, může „archivní bomba“ server zastavit.
Zadní vrátka	Trojské koně pro vzdálenou správu	Jsou považovány za nejnebezpečnější typ trojského koně. Z hlediska funkce se podobají aplikacím se vzdálenou správou, které jsou nainstalovány v počítači. Tyto programy se samy instalují do počítače, aniž by o tom uživatel věděl, takže útočník může počítač spravovat vzdáleně.
Trojský kůň	Trojské koně	Zahrnují následující škodlivé aplikace: • **Klasické trojské koně**. Tyto programy vykonávají pouze hlavní funkce trojských koňů: blokování, úpravu nebo ničení informací a zakazování počítačů nebo sítí. Nemají žádné pokročilé funkce, na rozdíl od trojských koňů popsaných v tabulce. • **Všestranné trojské koně**. Tyto programy mají rozšířené funkce typické pro několik typů trojských koňů.
Trojan-Ransom	Vyděračské trojské koně	Berou si údaje uživatele jako rukojmí, upravují je nebo blokují, nebo mají vliv na činnost počítače, takže uživatel ztratí možnost

		informace používat. Útočník požaduje od uživatele výkupné a slibuje zaslání aplikace pro obnovení výkonu počítače a dat, která v něm byla uložena.
Trojan-Clicker	Klikací trojské koně	Přistupují k webovým stránkám z počítače uživatele, odesláním příkazů do prohlížeče nebo změnou webových adres zadaných v souborech operačního systému. Použitím těchto programů útočníci páchají síťové útoky a zvyšují návštěvnost webů, čímž se zvyšuje počet zobrazení bannerových reklam.
Trojan-Downloader	Stahovací trojské koně	Přecházejí na webovou stránku útočníka, stahují z ní další škodlivé aplikace a instalují je do počítače uživatele. Mohou obsahovat název souboru škodlivé aplikace, která bude stažena nebo získána z webové stránky, kterou otevíráte.
Trojan-Dropper	Přetahovací trojské koně	Obsahují další trojské koně, které instalují na pevný disk. Útočníci mohou programy typu Trojan Dropper používat k následujícím účelům: • Instalovat škodlivou aplikaci, aniž by si toho uživatel všiml: Programy typu Trojan Dropper nezobrazují žádné zprávy, nebo zobrazují falešné zprávy, které informují například o chybě v archivu nebo nekompatibilní verzi operačního systému. • Chránit jiné škodlivé aplikace před nalezením: ne každý antivirový software může zjistit škodlivou aplikaci v rámci aplikace typu Trojan Dropper.
Trojan-Notifier	Oznamovací trojské koně	Informují útočníka, že infikovaný počítač je přístupný, a odesílají útočníkovi informace o počítači: IP adresa, počet otevřených portů nebo e-mailová adresa. S útočníkem se spojují prostřednictvím e-mailu, serveru FTP, přístupu na webovou stránku útočníka nebo jinak. Programy typu Trojan Notifier se často používají v sadách tvořených několika trojskými koni. Informují útočníka, že byly do počítače uživatele úspěšně nainstalovány jiné trojské koně.
Trojan-Proxy	Trojské koně proxy	Umožňují útočníkům anonymní přístup k webovým stránkám pomocí počítače uživatele. Často se používají k odesílání nevyžádané pošty.
Trojan-PSW	Trojské koně pro krádeže hesel	Trojské koně pro krádeže hesel, které kradou uživatelské účty, jako například registrační údaje k softwaru. Tyto trojské koně hledají důvěrná data v systémových souborech

		a registrech a odesílají je „veliteli“ e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak. Některé z těchto trojských koňů jsou kategorizovány jako samostatné typy, které jsou popsány v této tabulce. Tyto trojské koně kradou bankovní účty (Trojan-Banker), kradou data od uživatelů klientů IM (Trojan-IM) a informace od hráčů online her (Trojan-GameThief).
Trojan-Spy	Špionské trojské koně	Špehují uživatele a shromažďují informace o akcích, které uživatel provede během práce na počítači. Mohou zachytit data, která uživatel zadává na klávesnici, pořizovat jejich snímky nebo shromažďovat seznamy aktivních aplikací. Po získání informací je předají útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak.
Trojan-DDoS	Trojské koně – síťoví útočníci	Odesílají různé požadavky z počítače uživatele na vzdálený server. Server postrádá prostředky na zpracování všech požadavků, takže přestane fungovat (Denial of Service neboli DoS – odmítnutí služby). Hackeři často infikují řadu počítačů těmito programy, aby mohli počítače uživatelů využít k současnému útoku na jeden server. Programy DoS útočí z jednoho počítače s vědomím uživatele. Programy DDoS (distribuované DoS) vykonávají distribuované útoky z několika počítačů, aniž by si toho uživatel infikovaného počítače všiml.
Trojan-IM	Trojské koně, které kradou informace od uživatelů klientů IM	Kradou čísla a hesla účtů uživatelů klientů posílání rychlých zpráv. Předávají data útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak.
Rootkit	Rootkity	Maskují jiné škodlivé programy a jejich činnost, čímž prodlužují přítomnost aplikací v operačním systému. Rovněž ukrývají soubory, procesy v infikované paměti počítače nebo klíče registru, které spouští škodlivé aplikace. Rootkity mohou maskovat výměnu dat mezi aplikacemi v počítači uživatele a dalších počítačích v síti.
Trojan-SMS	Trojské koně v podobě zpráv SMS	Infikují mobilní telefony odesíláním zpráv SMS na telefonní čísla se sazbou za prémiové služby.
Trojan-GameThief	Trojské koně, které kradou informace od hráčů online her	Kradou přihlašovací údaje k účtům od hráčů online her a poté je odesílají útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak.

Trojan-Banker	Trojské koně, které kradou bankovní účty	Kradou údaje o bankovních účtech nebo data systémů elektronického bankovnictví a poté je odesílají hackerovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku hackera nebo jinou metodou.
Trojan-Mailfinder	Trojské koně, které shromažďují e-mailové adresy	Shromažďují e-mailové adresy, které ukládají do počítače, a odesílají je útočníkovi e-mailem, prostřednictvím serveru FTP, přechodem na webovou stránku útočníka nebo jinak. Útočníci mohou odesílat nevyžádanou poštu na adresy, které získali.

- Škodlivé nástroje

Podkategorie: Škodlivé nástroje

Úroveň nebezpečí: střední

Na rozdíl od jiných typů malwaru škodlivé nástroje neprovádějí své akce ihned po spuštění. Lze je v počítači uživatele bezpečně uložit a spustit. Útočníci často používají funkce těchto programů k vytváření virů, červů a trojských koňů, provádějí síťové útoky na vzdálených serverech, hackují počítače nebo provádějí jiné škodlivé akce.

Různé funkce škodlivých nástrojů jsou seskupeny dle typů popsaných v následující tabulce.

Funkce škodlivých nástrojů

Typ	Název	Popis
Konstruktor	Konstruktory	Umožňují vytváření nových virů, červů a trojských koňů. Některé konstruktory se chlubí standardním rozhraním se zobrazením v oknech, v nichž může uživatel vybrat typ škodlivé aplikace, který chce vytvořit, způsob boje s ladicími programy a další funkce.
Dos	Síťové útoky	Odesílají různé požadavky z počítače uživatele na vzdálený server. Server postrádá prostředky na zpracování všech požadavků, takže přestane fungovat (Denial of Service neboli DoS – odmítnutí služby).
Exploit	Exploity	Exploit je sada dat nebo programových kódů, která využívá zranitelnosti aplikace, ve které jsou zpracovány, a provádí v počítači škodlivou akci. Exploit může například zapisovat nebo číst soubory nebo požadovat infikované webové stránky. Různé exploity využívají zranitelnosti různých aplikací nebo síťových služeb. Exploit se tváří jako síťový paket a je přenášen sítí do několika počítačů, přičemž hledá počítače se zranitelnými síťovými službami. Exploit v souboru DOC využívá zranitelnosti textového editoru. Když uživatel otevře infikovaný soubor, může začít provádět akce, které jsou předprogramovány hackerem. Exploit vložený do e-mailové zprávy hledá zranitelnosti ve všech e-mailových klientech. Může začít provádět škodlivé akce, když uživatel otevře infikovanou zprávu v tomto e-mailovém klientovi. Červy Net-Worm se šíří v sítích pomocí exploitů. Nuker *exploity* jsou síťové pakety, které deaktivují počítače.
FileCryptor	Moduly pro šifrování	Šifrují jiné škodlivé aplikace a skrývají je před antivirovými aplikacemi.

Flooder	Programy pro kontaminaci sítí	Odesílají různé zprávy přes síťové kanály. Tento typ nástrojů zahrnuje například programy, které kontaminují systémy IRC (Internet Relay Chats). Nástroje typu Flooder nezahrnují programy, které kontaminují kanály používané e-mailem, klienty IM a systémy pro mobilní komunikaci. Tyto programy jsou samostatné typy popsané v tabulce (Email-Flooder, IM-Flooder a SMS-Flooder).
HackTool	Hackovací nástroje	Umožňují nabourat se do počítače, ve kterém jsou nainstalovány, nebo útočí na jiný počítač (například přidáním nových systémových účtů bez oprávnění uživatele nebo vymazáním protokolů systému za účelem zakrytí stop své přítomnosti v operačním systému). Tento typ nástrojů zahrnuje sledovací nástroje se škodlivými funkcemi, jako je například zachycení hesla. Sledovací programy umožňují zobrazení síťového provozu.
Hoax	Hoaxy	Varují uživatele zprávami o virech: mohou „zjistit virus“ v infikovaném souboru nebo informovat uživatele, že disk byl naformátován, ačkoli k tomu ve skutečnosti nedošlo.
Spoofer	Nástroje pro falšování adres	Odesílají zprávy a síťové požadavky s falešnou adresou odesilatele. Útočníci používají nástroje typu Spoofer například k tomu, aby byly považováni za skutečné odesilatele zpráv.
VirTool	Nástroje, které upravují škodlivé aplikace	Umožňují úpravu jiných malwarových programů, čímž je kryjí před antivirovými aplikacemi.
Email-Flooder	Programy, které kontaminují e-mailové adresy	Odesílají různé zprávy na různé e-mailové adresy, čímž je kontaminují. Velký objem příchozích zpráv brání uživatelům v zobrazení užitečných zpráv ve složce příchozích zpráv.
IM-Flooder	Programy, které kontaminují provoz klientů IM	Zaplavují uživatele klientů IM zprávami. Velký objem zpráv brání uživatelům v zobrazení užitečných příchozích zpráv.
SMS-Flooder	Programy, které kontaminují provoz zprávami SMS	Odesílají různé zprávy SMS na mobilní telefony.

- Adware

  Podkategorie: reklamní software (adware);

  Úroveň hrozby: střední

  Adware zobrazuje uživateli reklamní informace. Adwarové programy zobrazují bannerové reklamy v rozhraních jiných programů a přesměrovávají dotazy hledání na reklamní webové stránky. Některé z nich shromažďují marketingové informace o uživateli a odesílají je vývojáři: tyto informace mohou zahrnovat názvy webových stránek, které uživatel navštěvuje, nebo obsah dotazů hledání uživatele. Na rozdíl od programů typu Trojan-Spy adware odesílá informace vývojáři se souhlasem uživatele.

- Automatické vytáčení

Podkategorie: legální software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Úroveň nebezpečí: střední

Většina těchto aplikací je užitečná, takže je používá množství uživatelů. Tyto aplikace zahrnují klienty IRC, automatické vytáčení, programy pro stahování souborů, monitory aktivity počítačových systémů, nástroje pro správu hesel a internetové servery pro FTP, HTTP a Telnet.

Pokud však útočníci získají přístup k těmto programům nebo pokud je nasadí do počítače uživatele, mohou být některé funkce aplikace použity k narušení bezpečnosti.

Tyto aplikace se z hlediska funkcí liší. Jejich typy jsou popsány v následující tabulce.

Typ	Název	Popis
Client-IRC	Klienti internetových konverzací	Uživatelé instalují tyto programy, aby mohli komunikovat s lidmi v systému IRC (Internet Relay Chats). Útočníci je používají k šíření malwaru.
Dialer	Automatické vytáčení	Mohou navázat telefonická připojení přes modem ve skrytém režimu.
Downloader	Programy pro stahování	Mohou stahovat soubory z webových stránek ve skrytém režimu.
Monitor	Programy pro monitorování	Umožňují monitorování počítače, ve kterém jsou nainstalovány (zjištění, které aplikace jsou aktivní a jak si vyměňují data s aplikacemi nainstalovanými v jiných počítačích).
PSWTool	Nástroje pro obnovení hesla	Umožňují zobrazit a obnovit zapomenutá hesla. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem.
RemoteAdmin	Programy pro vzdálenou správu	Jsou často využívány správci systému. Tyto programy umožňují získat přístup k rozhraní vzdáleného počítače za účelem jeho sledování a správy. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem: monitorovat a spravovat vzdálené počítače. Legální programy pro vzdálenou správu se liší od trojských koňů typu Zadní vrátka pro vzdálenou správu. Trojské koně mohou proniknout do operačního systému nezávisle a nainstalovat se do něj. Legální programy to učinit nemohou.
Server-FTP	Servery FTP	Fungují jako servery FTP. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru FTP.
Server-Proxy	Proxy servery	Fungují jako proxy servery. Útočníci je

		nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
Server-Telnet	Servery Telnet	Fungují jako servery Telnet. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru Telnet.
Server-Web	Webové servery	Fungují jako webové servery. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru HTTP.
RiskTool	Nástroje pro práci na místním počítači	Poskytují uživateli další možnosti při práci s vlastním počítačem uživatele. Nástroje umožňují uživateli skrýt soubory nebo okna aktivních aplikací a ukončit aktivní procesy.
NetTool	Síťové nástroje	Poskytují uživateli další možnosti při práci s dalšími počítači v síti. Tyto nástroje umožňují jejich restart, zjištění otevřených portů a spuštění aplikací, které jsou v počítačích nainstalovány.
Client-P2P	Klienti sítě P2P	Umožňují práci v síti P2P. Útočníci je mohou používat k šíření malwaru.
Client-SMTP	Klienti SMTP	Odesílají e-mailové zprávy bez vědomí uživatele. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
WebToolbar	Webové panely nástrojů	Přidávají panely nástrojů do rozhraní jiných aplikací, aby bylo možné používat vyhledávače.
FraudTool	Pseudo programy	Vydávají se za jiné programy. Například existují pseudo antivirové programy, které zobrazují zprávy o zjištění malwaru. Ve skutečnosti však nic nenašly ani nedezinfikovaly.

- Zjišťovat další software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat

Podkategorie: legální software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Úroveň nebezpečí: střední

Většina těchto aplikací je užitečná, takže je používá množství uživatelů. Tyto aplikace zahrnují klienty IRC, automatické vytáčení, programy pro stahování souborů, monitory aktivity počítačových systémů, nástroje pro správu hesel a internetové servery pro FTP, HTTP a Telnet.

Pokud však útočníci získají přístup k těmto programům nebo pokud je nasadí do počítače uživatele, mohou být některé funkce aplikace použity k narušení bezpečnosti.

Tyto aplikace se z hlediska funkcí liší. Jejich typy jsou popsány v následující tabulce.

Typ	Název	Popis
Client-IRC	Klienti internetových konverzací	Uživatelé instalují tyto programy, aby mohli komunikovat s lidmi v systému IRC (Internet Relay Chats). Útočníci je používají k šíření malwaru.
Dialer	Automatické vytáčení	Mohou navázat telefonická připojení přes modem ve skrytém režimu.
Downloader	Programy pro stahování	Mohou stahovat soubory z webových stránek ve skrytém režimu.
Monitor	Programy pro monitorování	Umožňují monitorování počítače, ve kterém jsou nainstalovány (zjištění, které aplikace jsou aktivní a jak si vyměňují data s aplikacemi nainstalovanými v jiných počítačích).
PSWTool	Nástroje pro obnovení hesla	Umožňují zobrazit a obnovit zapomenutá hesla. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem.
RemoteAdmin	Programy pro vzdálenou správu	Jsou často využívány správci systému. Tyto programy umožňují získat přístup k rozhraní vzdáleného počítače za účelem jeho sledování a správy. Útočníci je tajně nasazují do počítačů uživatelů se stejným cílem: monitorovat a spravovat vzdálené počítače. Legální programy pro vzdálenou správu se liší od trojských koňů typu Zadní vrátka pro vzdálenou správu. Trojské koně mohou proniknout do operačního systému nezávisle a nainstalovat se do něj. Legální programy to učinit nemohou.
Server-FTP	Servery FTP	Fungují jako servery FTP. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru FTP.
Server-Proxy	Proxy servery	Fungují jako proxy servery. Útočníci je

		nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
Server-Telnet	Servery Telnet	Fungují jako servery Telnet. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru Telnet.
Server-Web	Webové servery	Fungují jako webové servery. Útočníci je nasazují do počítače uživatele za účelem otevření vzdáleného přístupu prostřednictvím serveru HTTP.
RiskTool	Nástroje pro práci na místním počítači	Poskytují uživateli další možnosti při práci s vlastním počítačem uživatele. Nástroje umožňují uživateli skrýt soubory nebo okna aktivních aplikací a ukončit aktivní procesy.
NetTool	Síťové nástroje	Poskytují uživateli další možnosti při práci s dalšími počítači v síti. Tyto nástroje umožňují jejich restart, zjištění otevřených portů a spuštění aplikací, které jsou v počítačích nainstalovány.
Client-P2P	Klienti sítě P2P	Umožňují práci v síti P2P. Útočníci je mohou používat k šíření malwaru.
Client-SMTP	Klienti SMTP	Odesílají e-mailové zprávy bez vědomí uživatele. Útočníci je nasazují do počítače uživatele za účelem otevření odesílání nevyžádané pošty jménem uživatelem.
WebToolbar	Webové panely nástrojů	Přidávají panely nástrojů do rozhraní jiných aplikací, aby bylo možné používat vyhledávače.
FraudTool	Pseudo programy	Vydávají se za jiné programy. Například existují pseudo antivirové programy, které zobrazují zprávy o zjištění malwaru. Ve skutečnosti však nic nenašly ani nedezinfikovaly.

- Komprimované objekty, jejichž komprimace může sloužit k ochraně škodlivého kódu

Aplikace Kaspersky Endpoint Security kontroluje komprimované objekty a rozbalovací modul v (samorozbalovacích) SFX archivech.

Aby bylo možné skrýt nebezpečné programy před antivirovými aplikacemi, útočníci je archivují pomocí speciálních komprimačních programů nebo vytvoří několikrát komprimované soubory.

Analytikové společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

Pokud aplikace Kaspersky Endpoint Security detekuje takový komprimační program v souboru, soubor pravděpodobně obsahuje škodlivou aplikaci nebo aplikaci, kterou lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Aplikace Kaspersky Endpoint Security rozlišuje následující typy programů:

- *Komprimované soubory, které mohou způsobit škodu* – používají se k balení malwaru, například virů, červů a trojských koňů.
- *Mnohonásobně komprimované soubory* (střední úroveň rizika) – objekt byl zkomprimován třikrát jedním nebo více komprimačními nástroji.

- **Mnohonásobně komprimované soubory**

Aplikace Kaspersky Endpoint Security kontroluje komprimované objekty a rozbalovací modul v (samorozbalovacích) SFX archivech.

Aby bylo možné skrýt nebezpečné programy před antivirovými aplikacemi, útočníci je archivují pomocí speciálních komprimačních programů nebo vytvoří několikrát komprimované soubory.

Analytikové společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

Pokud aplikace Kaspersky Endpoint Security detekuje takový komprimační program v souboru, soubor pravděpodobně obsahuje škodlivou aplikaci nebo aplikaci, kterou lze použít zločinným způsobem k poškození počítače nebo osobních dat.

Aplikace Kaspersky Endpoint Security rozlišuje následující typy programů:

- *Komprimované soubory, které mohou způsobit škodu* – používají se k balení malwaru, například virů, červů a trojských koňů.
- *Mnohonásobně komprimované soubory* (střední úroveň rizika) – objekt byl zkomprimován třikrát jedním nebo více komprimačními nástroji.

Výjimky

Tato tabulka obsahuje informace o výjimkách z kontroly.

Objekty můžete z kontroly vyloučit následujícími způsoby:

- Zadejte cestu k souboru nebo složce.
- Zadejte hodnotu hash objektu.

	• použitím masek:
	  • Hvězdičku `*`, která libovolnou skupinu znaků kromě znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\*\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách (nikoli však v podsložkách) na jednotce C.
	  • Dvě hvězdičky za sebou `*`, které v názvu souboru či složky zastupují libovolnou skupinu znaků (včetně prázdné skupiny), a to včetně znaků `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složce s názvem `Složka` a jejích podložkách. Maska musí obsahovat alespoň jednu úroveň vnoření. Maska `C:\**\*. Txt` není platná maska.
	  • Otazník `?`, který jeden libovolný znak kromě znaku `\` a `/` (tyto znaky slouží jako oddělovače názvů souborů a složek v cestách k souborům a složkám). Například maska `C:\Složka\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Složka`, které mají příponu TXT a název skládající se ze tří znaků.
	• Zadejte název typu objektu podle klasifikace encyklopedie Kaspersky (například `Email-Worm`, `Rootkit` nebo `RemoteAdmin`). Můžete použít masky se znakem `?` (nahradí libovolný jeden znak) a znakem `*` (nahradí libovolný počet znaků). Je-li například zadána maska `Client*`, aplikace Kaspersky Endpoint Security vyloučí z kontroly objekty `Client-IRC`, `Client-P2P` a `Client-SMTP`.

Důvěryhodné aplikace	Tato tabulka uvádí důvěryhodné aplikace, jejichž aktivita není aplikací Kaspersky Endpoint Security během činnosti monitorována. Součást Kontrola aplikací řídí spouštění všech aplikací, a to bez ohledu na skutečnost, zda je aplikace uvedena v tabulce důvěryhodných aplikací či nikoli.
Sloučit hodnoty při dědění *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Tím se sloučí seznam výjimek z kontroly a seznam důvěryhodných aplikací v nadřízených a podřízených zásadách aplikace Kaspersky Security Center. Chcete-li sloučit seznamy, podřízená zásada musí být nakonfigurována tak, aby zdědila nastavení nadřazené zásady aplikace Kaspersky Security Center. Pokud je zaškrtnuto toto políčko, položky seznamu z nadřazené zásady aplikace Kaspersky Security Center se zobrazí v podřízených zásadách. Tímto způsobem můžete například vytvořit konsolidovaný seznam důvěryhodných aplikací pro celou organizaci. Zděděné položky seznamu v podřízené zásadě nelze odstranit ani upravit. Položky v seznamu výjimek kontroly a seznamu důvěryhodných aplikací, které jsou sloučeny při dědění, lze odstranit a upravit pouze v nadřazené zásadě. Položky v zásadách nižší úrovně můžete přidávat, upravovat nebo odstraňovat. Pokud se položky v seznamech podřízené a nadřazené zásady shodují, zobrazí se tyto položky jako stejná položka nadřazených zásad. Není-li zaškrtávací políčko zaškrtnuto, položky seznamu se při dědění nastavení zásad Kaspersky Security Center nesloučí.
Povolit používání místních výjimek / Povolit používání místních	*Místní výjimky z kontroly a místní důvěryhodné aplikace (místní důvěryhodná zóna)* – uživatelsky definovaný seznam objektů a aplikací v aplikaci Kaspersky Endpoint Security pro konkrétní počítač. Aplikace Kaspersky Endpoint Security nesleduje objekty a aplikace z místní důvěryhodné zóny. Tímto způsobem mohou uživatelé kromě obecné důvěryhodné zóny v zásadách vytvářet také vlastní místní seznamy výjimek a důvěryhodných aplikací.

důvěryhodných aplikací *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Je-li toto políčko zaškrtnuto, může uživatel vytvořit místní seznam výjimek z kontroly a místní seznam důvěryhodných aplikací. Správce může pomocí aplikace Kaspersky Security Center zobrazit, přidat, upravit nebo odstranit položky seznamu ve vlastnostech počítače. Pokud políčko není zaškrtnuto, má uživatel přístup pouze k obecnému seznamu výjimek z kontroly a důvěryhodných aplikací generovanému v zásadách. Pokud byly vygenerovány místní seznamy, po deaktivaci této funkce aplikace Kaspersky Endpoint Security nadále vylučuje uvedené objekty z kontroly.
Úložiště důvěryhodných systémových certifikátů	Pokud je vybráno jedno z úložišť certifikátů důvěryhodného systému, aplikace Kaspersky Endpoint Security z kontroly vylučuje aplikace podepsané důvěryhodným digitálním podpisem. Kaspersky Endpoint Security automaticky přiřadí takové aplikace do skupiny *Důvěryhodné*. Pokud je vybrána možnost **Nepoužívat**, aplikace Kaspersky Endpoint Security kontroluje aplikace bez ohledu na to, zda mají digitální podpis. Aplikace Kaspersky Endpoint Security umísťuje aplikaci do skupiny důvěryhodnosti v závislosti na míře nebezpečí, které může tato aplikace pro počítač představovat.

Nastavení aplikace

Můžete nakonfigurovat následující obecná nastavení aplikace:

- Režim operace
- Sebeobrana
- Výkon
- Informace o ladění
- Stav počítače při používání nastavení

Nastavení aplikace

Parametr	Popis
Spouštět aplikaci Kaspersky Endpoint Security při spuštění počítače	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security se spustí po načtení operačního systému, čímž počítač chrání během celé relace. Pokud toto políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security se nespustí po načtení operačního systému, dokud ji uživatel nespustí ručně. Ochrana počítače je zakázána a data uživatele mohou být vystavena hrozbám.
Povolit technologii pokročilé dezinfekce	Pokud je políčko zaškrtnuté, při zjištění škodlivé aktivity v operačním systému se na obrazovce zobrazí místní oznámení. V oznámení aplikace Kaspersky Endpoint Security nabízí uživateli provedení pokročilé dezinfekce počítače. Jakmile uživatel tento postup schválí, aplikace Kaspersky Endpoint Security hrozbu zneutralizuje. Po dokončení postupu pokročilé dezinfekce aplikace Kaspersky Endpoint Security restartuje počítač. Technologie pokročilé dezinfekce využívá značné množství výpočetních prostředků, což může jiné aplikace zpomalovat.

	Je-li aplikace Kaspersky Endpoint Security nainstalována v počítači se systémem Windows pro servery, toto upozornění nezobrazí. Uživatel tak nemůže vybrat akci, která dezinfikuje aktivní hrozbu. Chcete-li dezinfikovat hrozbu, musíte v nastavení aplikace povolit technologii pokročilé dezinfekce a v nastavení úlohy *Antivirová kontrola* spustit pokročilou dezinfekci okamžitě. Poté musíte spustit úlohu *Antivirová kontrola*.
Použít Kaspersky Security Center jako proxy server pro aktivaci *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Je-li toto políčko zaškrtnuto, server pro správu aplikace Kaspersky Security Center bude použit jako proxy server při aktivace aplikace.
Povolit sebeobranu	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security brání úpravám nebo odstranění souborů aplikace na pevném disku, paměťových procesů a záznamů v systémovém registru.
Povolit správu nastavení aplikace Kaspersky Endpoint Security pomocí aplikací pro vzdálenou správu	Pokud je toto políčko zaškrtnuté, mohou nastavení aplikace Kaspersky Endpoint Security měnit důvěryhodné aplikace pro vzdálenou správu (například TeamViewer, LogMeIn Pro a Remotely Anywhere). Nedůvěryhodné aplikace pro vzdálenou správu mají zakázáno upravovat nastavení aplikace Kaspersky Endpoint Security, i když je zaškrtnuto toto políčko.
Povolit vnější řízení služby	Je-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security povolí všechny pokusy o správu služeb aplikace ze vzdáleného počítače. Pokud dojde k pokusu o vzdálenou správu služeb aplikace, na hlavním panelu systému Microsoft Windows nad ikonou aplikace se zobrazí oznámení (pokud nebyla oznamovací služba vypnuta uživatelem).
Odložit naplánované úlohy při napájení z baterie	Pokud je toto políčko zaškrtnuto, je režim úspory energie povolen. Aplikace Kaspersky Endpoint Security plánované úlohy odloží. Úlohy kontroly a aktualizace můžete spustit ručně, je-li třeba.
Při zatížení přenechat zdroje ostatním aplikacím	Když aplikace Kaspersky Endpoint Security spustí plánované úlohy, může dojít ke zvýšenému zatížení procesoru a podsystémů disku, což může mít dopad na výkon ostatních aplikací. Když je toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security odloží plánované úlohy, jakmile zjistí zvýšené zatížení, a uvolní prostředky operačního systému pro uživatelské aplikace.
Povolit zápis výpisu paměti	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security zapíše výpisy paměti, když dojde k jejímu pádu.

	Není-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezapíše výpisy paměti. Aplikace také odstraní existující soubory výpisu paměti z pevného disku počítače.
Povolit ochranu souborů výpisu a trasování	Je-li toto políčko zaškrtnuto, přístup k souborům výpisu je udělen správci systému a místnímu správci a také uživateli, který povolil zápis souborů výpisu nebo trasování. K souborům trasování mají přístup pouze správci systému a místní správci. Pokud toto políčko není zaškrtnuté, může k souborům výpisu a trasování přistupovat jakýkoli uživatel.
Stav počítače při používání nastavení *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Nastavení zobrazení stavů klientských počítačů s nainstalovanou aplikací Kaspersky Endpoint Security ve webové konzoli v případě, že při použití zásady nebo spuštění úlohy dojde k chybám. K dispozici jsou stavy *OK*, *Varování*, a *Kritické*.

Zprávy a úložiště

Zprávy

Ve zprávách jsou zaznamenávány informace o provozu každé součásti aplikace Kaspersky Endpoint Security, událostech šifrování dat, provedení každé úlohy kontroly, úlohy aktualizace, úlohy kontroly integrity a také o celkovém fungování aplikace.

Zprávy jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES\Report`.

Záloha

Funkce *zálohování* ukládá záložní kopie souborů, které byly odstraněny nebo změněny během dezinfekce. *Záložní kopie* je kopie souboru vytvořená, předtím než byl soubor dezinfikován nebo odstraněn. Záložní kopie souborů jsou ukládány ve zvláštním formátu a nepředstavují hrozbu.

Záložní kopie souborů jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES\QB`.

Uživatelům ve skupině správců je uděleno úplné oprávnění pro přístup k této složce. Uživateli, jehož účet byl použit k instalaci aplikace Kaspersky Endpoint Security, jsou udělena omezená přístupová práva k této složce.

Aplikace Kaspersky Endpoint Security neposkytuje možnost konfigurace přístupových oprávnění uživatele za účelem zálohování kopií souborů.

Nastavení zpráv a úložiště

Parametr	Popis
Neukládat zprávy	Pokud je toto políčko zaškrtnuto, maximální doba ukládání sestav je omezena na definovaný časový interval. Výchozí maximální doba uchovávání zpráv je 30 dní. Po této době bude

déle než N dny/dnů	aplikace Kaspersky Endpoint Security automaticky mazat nejstarší záznamy ze souboru zprávy.
Omezit velikost souboru zprávy na N MB	Pokud je toto políčko zaškrtnuto, maximální velikost souboru sestavy je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost souboru nastavena na 1024 MB. Aby nedošlo k překročení maximální velikosti souboru zprávy, bude aplikace Kaspersky Endpoint Security po dosažení maximální velikosti automaticky mazat nejstarší záznamy.
Neukládat objekty déle než N dny/dnů	Pokud je toto políčko zaškrtnuto, maximální doba ukládání souborů je omezena na definovaný časový interval. Výchozí maximální doba uložení souborů je 30 dní. Po uplynutí maximální doby uložení aplikace Kaspersky Endpoint Security nejstarší soubory ze složky záloh odstraní.
Omezit velikost zálohy na N MB	Pokud je toto políčko zaškrtnuto, maximální velikost úložiště je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost nastavena na 100 MB. Aby nedošlo k překročení maximální velikosti úložiště, bude aplikace Kaspersky Endpoint Security po dosažení maximální velikosti úložiště automaticky z úložiště odstraňovat nejstarší soubory.
Přenos dat na server pro správu *(k dispozici pouze v aplikaci Kaspersky Security Center)*	Kategorie událostí v klientských počítačích, jejichž informace je nutné předávat serveru pro správu.

Nastavení sítě

Můžete nakonfigurovat proxy server používaný pro připojení k internetu a aktualizaci antivirových databází, vybrat režim monitorování síťových portů a nakonfigurovat kontrolu šifrovaných připojení.

Možnosti sítě

Parametr	Popis
Omezit provoz u měřených připojení	Pokud je toto políčko zaškrtnuté, aplikace sníží síťový provoz při omezeném připojení k internetu. Aplikace Kaspersky Endpoint Security rozpozná vysokorychlostní mobilní připojení k Internetu jako omezené připojení, zatímco Wi-Fi připojení rozpozná jako neomezené připojení. Provoz sítě s ohledem na náklady funguje na počítačích se systémem Windows 8 nebo novějším.
Vložit skript do síťového provozu za účelem interakce s webovými stránkami	Pokud je políčko zaškrtnuto, aplikace Kaspersky Endpoint Security vloží do webového provozu skript pro interakci s webovými stránkami. Tento skript zajišťuje, že součást Kontrola webu může pracovat správně. Skript umožňuje registraci událostí součásti Kontrola webu. Bez tohoto skriptu nemůžete povolit sledování aktivity uživatele na internetu. Odborníci společnosti Kaspersky doporučují vložit tento skript pro interakci s webovými stránkami do provozu, aby byla zajištěna správná funkce součásti Kontrola webu.
Proxy server	Nastavení proxy serveru, který se použije pro přístup uživatelů klientských počítačů

	k internetu. Aplikace Kaspersky Endpoint Security používá tato nastavení pro určité součásti ochrany, včetně aktualizace databází a modulů aplikace. Pro automatickou konfiguraci proxy serveru použije aplikace Kaspersky Endpoint Security protokol WPAD (Web Proxy Auto-Discovery Protocol). Pokud nelze IP adresu proxy serveru pomocí tohoto protokolu určit, aplikace Kaspersky Endpoint Security použije adresu proxy serveru zadanou v nastavení prohlížeče Microsoft Internet Explorer.
Nepoužívat proxy server pro adresy vnitřní sítě	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nepoužije proxy serveru při provádění aktualizace ze sdílené složky.
Sledované porty	**Sledovat všechny síťové porty**. V tomto režimu sledování síťových portů součásti ochrany (Ochrana před souborovými hrozbami, Ochrana před webovými hrozbami, Ochrana před hrozbami v poště) sledují datové proudy, které jsou přenášeny prostřednictvím jakýchkoli otevřených síťových portů počítače. **Sledovat pouze vybrané síťové porty**. V tomto režimu monitorování síťových portů sledují součásti ochrany vybrané porty počítače a síťovou aktivitu vybraných aplikací. Seznam síťových portů, které se obvykle používají k přenosu elektronické pošty a síťového provozu, se konfiguruje podle doporučení odborníků společnosti Kaspersky. **Sledovat všechny porty aplikací ze seznamu doporučeného společností Kaspersky**. Tato funkce využívá předdefinovaný seznam aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security. Tento seznam zahrnuje například Google Chrome, Adobe Reader, Java a další aplikace. **Sledovat všechny porty u zadaných aplikací**. Tato funkce používá seznam aplikací, jejichž síťové porty jsou monitorovány aplikací Kaspersky Endpoint Security.
Kontrola šifrovaného připojení	Kaspersky Endpoint Security kontroluje šifrovaný síťový provoz přenášený přes následující protokoly: • SSL 3.0. • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Aplikace Kaspersky Endpoint Security podporují následující režimy kontroly síťového provozu: • **Nekontrolovat šifrovaná připojení** Aplikace Kaspersky Endpoint Security nebude mít přístup k obsahu webů, jejichž adresa začíná na `https://`. • **Kontrolovat šifrovaná připojení na žádost odeslanou součástmi ochrany**. Aplikace Kaspersky Endpoint Security bude kontrolovat šifrované přenosy, pouze pokud o to požádají součásti Ochrana před souborovými hrozbami, Ochrana před hrozbami v poště nebo Kontrola webu. • **Vždy kontrolovat šifrovaná připojení** Aplikace Kaspersky Endpoint Security bude kontrolovat šifrovaný provoz, i když jsou zakázány součásti ochrany.

	Aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení vytvořená důvěryhodnými aplikacemi, pro které je kontrola provozu zakázána. Aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení z předdefinovaného seznamu důvěryhodných webů. Předdefinovaný seznam důvěryhodných webů vytvářejí odborníci společnosti Kaspersky. Tento seznam je aktualizován o antivirové databáze aplikace. Předdefinovaný seznam důvěryhodných webů můžete zobrazit pouze v rozhraní aplikace Kaspersky Endpoint Security. Seznam nemůžete zobrazit v konzole aplikace Kaspersky Security Center.
Při návštěvě domény s nedůvěryhodným certifikátem	• **Povolit**. Pokud je vybrána tato možnost, při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security povolí síťové připojení. Při otevření domény s nedůvěryhodným certifikátem v prohlížeči zobrazí aplikace Kaspersky Endpoint Security stránku HTML s upozorněním a důvodem toho, proč není návštěva dané domény doporučena. Uživatel může kliknout na odkaz na stránce HTML s upozorněním, aby získal přístup k požadovanému webovému prostředku. Po přejití na odkaz nebude aplikace Kaspersky Endpoint Security během další hodiny v případě návštěvy jiných prostředků v této stejné doméně zobrazovat upozornění na nedůvěryhodný certifikát. • **Blokovat připojení**. Pokud je vybrána tato možnost, při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security blokuje síťové připojení. Při otevření domény s nedůvěryhodným certifikátem v prohlížeči zobrazí aplikace Kaspersky Endpoint Security stránku HTML s důvodem toho, proč je daná doména blokována.
Při výskytu chyb kontroly šifrovaného připojení	• **Blokovat připojení**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení blokuje síťové připojení. • **Přidat doménu do výjimek**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení přidá doménu, v jejímž důsledku došlo k chybě, do seznamu výjimek s chybami kontroly a při návštěvě této domény nesleduje šifrovaný síťový provoz. Seznam domén s chybami kontroly šifrovaného připojení můžete zobrazit pouze v místním rozhraní aplikace. Chcete-li vymazat obsah seznamu, musíte vybrat možnost **Blokovat připojení**.
Blokovat připojení SSL 2.0	Pokud je políčko zaškrtnuto, aplikace Kaspersky Endpoint Security blokuje síťová připojení vytvořená pomocí protokolu SSL 2.0. Pokud políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security neblokuje síťová připojení vytvořená pomocí protokolu SSL 2.0 a nesleduje síťový provoz přenášený pomocí těchto připojení.
Dešifrovat šifrovaná připojení u webů používajících certifikáty EV	Certifikáty EV (Extended Validation Certificate) potvrzují pravost webových stránek a zvyšují bezpečnost připojení. K označení, že web má certifikát EV, používají prohlížeče ikonu zámku v adresním řádku. Prohlížeče mohou pruh adresy také plně nebo částečně vybarvit zelenou barvou. Pokud je toto políčko zaškrtnuté, aplikace Kaspersky Endpoint Security dešifruje a monitoruje šifrovaná připojení a weby, které používají certifikát EV.

	Jestliže toto políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security nemá přístup k obsahu provozu HTTPS. Z tohoto důvodu aplikace monitoruje provoz HTTPS pouze na základě adresy webových stránek, například, `https://facebook.com`. Pokud poprvé otevíráte web s certifikátem EV, šifrované připojení bude dešifrováno bez ohledu na to, zda je toto políčko zaškrtnuto.
Důvěryhodné adresy	Tato funkce používá seznam webových adres, u kterých aplikace Kaspersky Endpoint Security nekontroluje síťová připojení. Můžete zadat název domény nebo IP adresu. Kaspersky Endpoint Security podporuje při zadávání masky názvu domény znak `*`. Aplikace Kaspersky Endpoint Security nepodporuje masky pro IP adresy. Příklady: • `domena.cz` – tato položka zahrnuje následující adresy: `https://domena.cz`, `https://www.domena.cz`, `https://domena.cz/stranka123`. Tato položka nezahrnuje subdomény (například, `subdomena.domena.cz`). • `subdomena.domena.cz` – tato položka zahrnuje následující adresy: `https://subdomena.domena.cz`, `https://subdomena.domena.cz/stranka123`. Tato položka nezahrnuje doménu `domena.cz`. • `*.domena.cz` – tato položka zahrnuje následující adresy: `https://filmy.domena.cz`, `https://obrazky.domena.cz/stranka123`. Tato položka nezahrnuje doménu `domena.cz`.
Důvěryhodné aplikace	Seznam aplikací, jejichž aktivita není aplikací Kaspersky Endpoint Security během činnosti sledována. Můžete vybrat typy aktivit aplikací, které aplikace Kaspersky Endpoint Security nebude sledovat (například nekontrolovat síťový provoz). Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
Kontrolovat zabezpečené přenosy v aplikacích Mozilla *(k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security)*	Pokud je toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security kontroluje šifrovaný provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird. Přístup k některým webovým stránkám přes protokol HTTPS může být zablokovaný. Chcete-li kontrolovat provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird, musíte povolit kontrolu šifrovaného připojení. Je-li kontrola šifrovaného připojení zakázána, aplikace Kaspersky Endpoint Security nekontroluje šifrovaný provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird. Aplikace Kaspersky Endpoint Security používá k dešifrování a analýze šifrovaného provozu kořenový certifikát Kaspersky. Můžete vybrat úložiště certifikátů, které bude obsahovat kořenový certifikát Kaspersky. • **Použít úložiště certifikátů Windows**. Kořenový certifikát společnosti Kaspersky bude přidán do tohoto úložiště během instalace aplikace Kaspersky Endpoint Security. • **Použít úložiště certifikátů prohlížeče Mozilla**. Mozilla Firefox a Thunderbird používají svá vlastní úložiště certifikátů. Pokud je vybráno úložiště certifikátů Mozilla, musíte do tohoto úložiště ručně přidat kořenový certifikát společnosti Kaspersky prostřednictvím vlastností prohlížeče.

Rozhraní

Můžete nakonfigurovat nastavení rozhraní aplikace.

Nastavení rozhraní

Parametr	Popis
Interakce s uživatelem *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	**Se zjednodušeným rozhraním**. V klientském počítači je hlavní okno aplikace nepřístupné a je k dispozici pouze ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel s aplikací Kaspersky Endpoint Security provádět omezený počet operací. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace. **S úplným rozhraním**. V klientském počítači je k dispozici hlavní okno aplikace Kaspersky Endpoint Security a ikona v oznamovací oblasti systému Windows. V místní nabídce ikony může uživatel provádět operace s aplikací Kaspersky Endpoint Security. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace. **Žádné rozhraní**. V klientském počítači se nezobrazují žádné známky provozu aplikace Kaspersky Endpoint Security. Ikona v oznamovací oblasti systému Windows ani upozornění nejsou k dispozici.
Nastavení upozornění	Tabulka s nastaveními oznámení o událostech s různými úrovněmi důležitosti, ke kterým může dojít během činnosti součásti, úlohy nebo celé aplikace. Aplikace Kaspersky Endpoint Security zobrazí oznámení o těchto událostech na obrazovce, odešle je e-mailem nebo je zaznamená do protokolu.
Nastavení upozornění elektronickou poštou	Nastavení SMTP serveru pro doručování upozornění na události zjištěné během provozu aplikace.
Zobrazení stavu aplikace v oznamovací oblasti	Kategorií událostí aplikací, které způsobí změnu ikony aplikace Kaspersky Endpoint Security v oznamovací oblasti hlavního panelu systému Microsoft Windows (nebo) a jejichž výsledkem je místní oznámení.
Upozornění týkající se stavu místní antivirové databáze	Nastavení oznámení o zastaralých antivirových databázích použitých aplikací.
Ochrana heslem	Je-li přepínací tlačítko v zapnuté poloze, aplikace Kaspersky Endpoint Security vyzve uživatele k zadání hesla, když se uživatel pokusí provést operaci, která spadá do oblasti ochrany heslem. Rozsah ochrany heslem zahrnuje zakázané operace (například zakázání součástí ochrany) a uživatelské účty, které jsou součástí rozsahu ochrany heslem. Po zapnutí ochrany heslem vás aplikace Kaspersky Endpoint Security vyzve k nastavení hesla pro provádění operací.
Webové prostředky technické podpory	Seznam odkazů na webové prostředky s informacemi o technické podpoře pro aplikaci Kaspersky Endpoint Security. Přidané odkazy se zobrazují v okně **Podpora** v místním rozhraní aplikace Kaspersky Endpoint Security namísto standardních odkazů.

(k dispozici pouze v konzole aplikace Kaspersky Security Center)	
Zpráva pro uživatele *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Zpráva, která se zobrazí v okně **Podpora** místního rozhraní aplikace Kaspersky Endpoint Security.

Správa nastavení

Aktuální nastavení aplikace Kaspersky Endpoint Security můžete uložit do souboru a použít je k rychlé konfiguraci aplikace na jiném počítači. Konfigurační soubor můžete použít také při nasazování aplikace prostřednictvím aplikace Kaspersky Security Center 12 pomocí instalačního balíčku. Výchozí nastavení můžete kdykoli obnovit.

Nastavení správy konfigurace aplikace je k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security.

Nastavení správy konfigurace aplikace

Nastavení	Popis
Importovat	Slouží k extrakci nastavení aplikace ze souboru ve formátu CFG a jeho použití.
Exportovat	Slouží k uložení aktuálního nastavení aplikace do souboru ve formátu CFG.
Obnovit	Nastavení doporučené společností Kaspersky pro aplikaci Kaspersky Endpoint Security můžete kdykoli obnovit. Po obnovení nastavení bude pro všechny součásti ochrany nastavena **doporučená** úroveň zabezpečení.

Správa úloh

Můžete vytvářet následující typy úloh pro správu aplikace Kaspersky Endpoint Security prostřednictvím rozhraní Kaspersky Security Center:

- místní úlohy, které jsou nakonfigurovány pro jeden klientský počítač;
- skupinové úlohy, které jsou nakonfigurovány pro klientské počítače v rámci skupin správy;
- Úlohy pro výběr počítačů.

Můžete vytvořit libovolný počet skupinových úloh, úloh pro výběr počítačů nebo místních úloh. Podrobnější informace o práci se skupinami pro správu a výběru počítačů najdete v *nápovědě k aplikaci Kaspersky Security Center*.

Nastavení správy úloh

Parametr	Popis
Povolit použití místních úloh	Je-li toto políčko zaškrtnuto, místní úlohy se zobrazí v místním rozhraní aplikace Kaspersky Endpoint Security. Pokud neexistují žádná další omezení zásad, uživatel může úlohy nakonfigurovat a spustit. Konfigurace plánu spouštění úlohy však pro uživatele zůstává nedostupná. Uživatel může úlohy spouštět pouze ručně. Pokud toto políčko není zaškrtnuté, použití místních úloh je zastaveno. V tomto režimu se místní úlohy nespouští dle plánu. Úlohy nelze spustit ani nakonfigurovat v místním rozhraní aplikace Kaspersky Endpoint Security ani při práci s příkazovým řádkem. Uživatel může antivirovou kontrolu souboru nebo složky přesto spustit výběrem možnosti **Zkontrolovat na výskyt virů** v místní nabídce souboru nebo složky. Úloha kontroly se spustí s výchozími hodnotami nastavení pro vlastní Uživatelská kontrola.
Povolit zobrazení úloh skupiny	Je-li toto políčko zaškrtnuto, úlohy skupiny se zobrazí v místním rozhraní aplikace Kaspersky Endpoint Security. Uživatel si může zobrazit seznam všech úloh v rozhraní aplikace. Pokud políčko zaškrtnuto není, aplikace Kaspersky Endpoint Security zobrazí prázdný seznam úloh.
Povolit správu úloh skupiny	Pokud je políčko zaškrtnuté, uživatelé mohou spouštět a zastavovat úlohy skupiny uvedené v aplikaci Kaspersky Security Center. Uživatelé mohou spouštět a zastavovat úlohy v rozhraní aplikace nebo ve zjednodušeném rozhraní aplikace. Pokud políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security bude naplánované úlohy spouštět automaticky nebo správce bude úlohy spouštět ručně v aplikaci Kaspersky Security Center.

Kontrola počítače

Antivirová kontrola je zásadní pro bezpečnost počítače. Pravidelně provádějte antivirovou kontrolu, abyste zabránili šíření malwaru, který nebyl zjištěn součástmi ochrany z důvodu nízkého nastavení úrovně zabezpečení nebo z jiných důvodů.

Aplikace Kaspersky Endpoint Security nekontroluje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive, a vytváří položky protokolu, které uvádějí, že tyto soubory nebyly prohledány.

Úplná kontrola

Důkladně zkontroluje celý počítač. Aplikace Kaspersky Endpoint Security kontroluje tyto objekty:

- paměť jádra;
- objekty načítané při spouštění operačního systému;
- spouštěcí sektory;
- zálohu operačního systému;
- všechny pevné disky a vyměnitelné jednotky.

Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Úplná kontrola*.

Chcete-li ušetřit prostředky počítače, místo úlohy úplné kontroly se doporučuje spustit úlohu kontroly na pozadí. Neovlivní to úroveň zabezpečení počítače.

Kontrola kritických oblastí

Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků.

Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Kontrola kritických oblastí*.

Vlastní kontrola

Aplikace Kaspersky Endpoint Security kontroluje objekty, které vybral uživatel. Můžete kontrolovat kterýkoli objekt na tomto seznamu:

- paměť jádra;
- objekty načítané při spouštění operačního systému;
- zálohu operačního systému;
- Poštovní schránka aplikace Outlook;
- pevné, vyměnitelné a síťové jednotky;
- jakýkoli vybraný soubor.

Kontrola na pozadí

Kontrola na pozadí je režim kontroly aplikace Kaspersky Endpoint Security, který uživateli nezobrazuje oznámení. Kontrola na pozadí vyžaduje méně prostředků počítače než jiné typy kontrol (například úplná kontrola). V tomto režimu aplikace Kaspersky Endpoint Security kontroluje spouštěcí objekty, spouštěcí sektor, systémovou paměť a systémový oddíl.

Kontrola integrity

Aplikace Kaspersky Endpoint Security zkontroluje moduly aplikace z hlediska změn nebo poškození.

Nastavení kontroly

Parametr	Popis
Úroveň zabezpečení	Aplikace Kaspersky Endpoint Security může pro spuštění kontroly použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy v aplikaci, se nazývají *úrovně zabezpečení*. • **Vysoká**. Aplikace Kaspersky Endpoint Security kontroluje všechny typy souborů. Při kontrole složených souborů může aplikace Kaspersky Endpoint Security kontrolovat

	i soubory formátu e-mailu. • **Doporučená**. Aplikace Kaspersky Endpoint Security kontroluje pouze vybrané formáty souborů na všech pevných discích, síťových discích a vyměnitelných úložných médiích počítače a také vložené objekty OLE. Aplikace Kaspersky Endpoint Security nekontroluje archivy ani instalační balíčky. • **Nízká**. Aplikace Kaspersky Endpoint Security kontroluje pouze nové nebo upravené soubory s vybranými příponami na všech pevných discích, vyměnitelných jednotkách a síťových discích počítače. Aplikace Kaspersky Endpoint Security nekontroluje složené soubory.
Akce při zjištění hrozby	**Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb. **Informovat**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb. Před pokusem o dezinfekci nebo odstranění infikovaného souboru vytvoří aplikace Kaspersky Endpoint Security záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.
Rozsah ochrany	Seznam objektů, které aplikace Kaspersky Endpoint Security kontroluje při provádění úlohy kontroly. Objekty v rozsahu kontroly mohou zahrnovat paměť jádra, běžící procesy, spouštěcí sektory, úložiště pro zálohu systému, poštovní databáze, pevný disk, vyměnitelný nebo síťový disk, složku nebo soubor.
Plán kontrol	**Ručně**. Režim spuštění, ve kterém můžete kontrolu spustit ručně v době, kdy je to pro vás výhodné. **Naplánováno**. V tomto režimu spuštění úlohy kontroly bude aplikace Kaspersky Endpoint Security spouštět úlohu kontroly podle vytvořeného plánu. Pokud je vybrán tento režim spuštění úlohy kontroly, je možné úlohu kontroly spustit i ručně.
Spustit neprovedené úlohy *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu kontroly, jakmile to bude možné. Úlohu kontroly lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy kontroly. Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security vynechané úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu kontroly.
Spustit pouze v době, kdy je počítač neaktivní	Odložené spuštění úlohy kontroly, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky.
Spustit	Ve výchozím nastavení je úloha kontroly spuštěna pod jménem uživatele, s jehož právy jste

kontrolu jako	zaregistrováni v operačním systému. Rozsah ochrany může zahrnovat síťové jednotky nebo jiné objekty, které vyžadují zvláštní přístupová práva. Můžete zadat uživatele, který má požadovaná práva v nastavení úlohy kontroly, a úlohu kontroly spustit pod účtem tohoto uživatele.
Typy souborů	Aplikace Kaspersky Endpoint Security považuje soubory bez přípony za spustitelné soubory. Aplikace Kaspersky Endpoint Security vždy kontroluje spustitelné soubory, bez ohledu na typy souborů, které pro kontrolu vyberete. **Všechny soubory**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje všechny soubory bez výjimky (všechny formáty a přípony). **Soubory kontrolované podle formátu**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví soubory, aby bylo možné určit formát souboru (například TXT, DOC nebo EXE). Kontrola také hledá soubory s konkrétními příponami. **Soubory kontrolované podle přípony**. Je-li toto nastavení povoleno, aplikace Kaspersky Endpoint Security zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.
Kontrolovat pouze nové a změněné soubory	Kontroluje pouze nové soubory a soubory, které byly od posledního skenování změněny. To pomáhá zkrátit dobu skenování. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.
Přeskočit soubory, které se kontrolují déle než N s	Omezí dobu trvání kontroly jednoho objektu. Po zadané době aplikace Kaspersky Endpoint Security ukončí kontrolu souboru. To pomáhá zkrátit dobu skenování.
Kontrolovat archivy	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
Kontrolovat distribuční balíčky	Toto políčko povolí nebo zakáže kontrolu distribučních balíčků třetích stran.
Kontrolovat soubory ve formátu aplikací Microsoft Office	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Skenovat formáty e-mailů	Tímto zaškrtávacím políčkem povolíte nebo zakážete možnost, na jejímž základě aplikace Kaspersky Endpoint Security kontroluje soubory ve formátech e-mailu a e-mailové databáze. Aplikace plně kontroluje pouze formáty souborů MS Outlook, Windows Mail / Outlook Express a EML a pouze v případě, že počítač má poštovního klienta MS Outlook x86. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security rozdělí soubor v e-mailovém formátu na jednotlivé komponenty (záhlaví, zpráva, přílohy) a zkontroluje, zda neobsahují hrozby. Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security zkontroluje soubor e-mailového formátu jako jeden soubor.
Kontrolovat	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security zkontroluje archivy

archivy chráněné heslem	chráněné heslem. Než bude možné soubory v archivu zkontrolovat, budete vyzváni k zadání hesla. Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security přeskočí kontrolu archivů chráněných heslem.
Nerozbalovat velké složené soubory	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace Kaspersky Endpoint Security zkontroluje složené soubory všech velikostí. Aplikace Kaspersky Endpoint Security kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.
Strojové učení a analýza signatur	Metoda strojového učení a analýzy signatur používá databáze aplikace Kaspersky Endpoint Security, které obsahují popisy známých hrozeb a způsoby jejich neutralizace. Ochrana využívající tuto metodu poskytuje minimální přijatelnou úroveň zabezpečení. Na základě doporučení odborníků společnosti Kaspersky je metoda strojového učení a analýzy signatur vždy povolena.
Heuristická analýza	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Technologie iSwift	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.
Technologie iChecker	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).

Kontrola na pozadí

Kontrola na pozadí je režim kontroly aplikace Kaspersky Endpoint Security, který uživateli nezobrazuje oznámení. Kontrola na pozadí vyžaduje méně prostředků počítače než jiné typy kontrol (například úplná kontrola). V tomto režimu aplikace Kaspersky Endpoint Security kontroluje spouštěcí objekty, spouštěcí sektor, systémovou paměť a systémový oddíl. Kontrola na pozadí se spustí v následujících případech:

- Po dokončení aktualizace antivirové databáze.
- 30 minut po spuštění aplikace Kaspersky Endpoint Security.
- Každých šest hodin.
- Když je počítač nečinný po dobu pěti nebo více minut (počítač je uzamčen nebo je zapnutý spořič obrazovky).

Testování na pozadí, když je počítač nečinný, je přerušeno, pokud jsou splněny některé z následujících podmínek:

- Počítač přešel do aktivního režimu.

  Pokud skenování na pozadí nebylo spuštěno déle než deset dní, skenování nebude přerušeno.

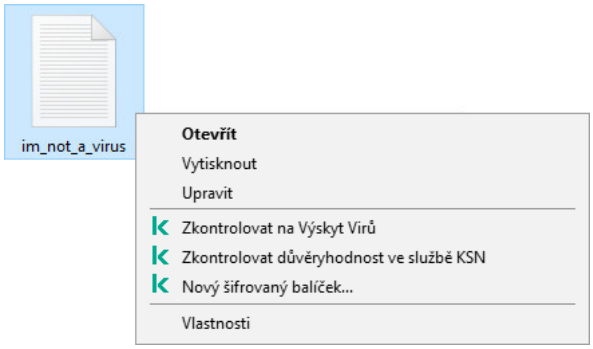
- Počítač (notebook) se přepnul do režimu napájení z baterie.

Při provádění kontroly na pozadí aplikace Kaspersky Endpoint Security nekontroluje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive.

Kontrola z místní nabídky

Aplikace Kaspersky Endpoint Security umožňuje z místní nabídky spustit kontrolu výskytu virů a jiného malwaru v jednotlivých souborech (viz obrázek níže).

Při provádění kontroly z místní nabídky aplikace Kaspersky Endpoint Security nekontroluje soubory, jejichž obsah je umístěn v cloudovém úložišti OneDrive.



Kontrola z místní nabídky

Nastavení úlohy Kontrola z místní nabídky

Parametr	Popis
Akce při zjištění hrozby	**Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory odstraní. **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Je-li tato možnost vybrána, aplikace Kaspersky Endpoint Security se automaticky pokusí dezinfikovat všechny nalezené infikované soubory. Pokud není dezinfekce možná, aplikace Kaspersky Endpoint Security přidá informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb. **Informovat**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security přidá při zjištění infikovaných souborů informace o těchto souborech do seznamu aktivních hrozeb.
Kontrolovat pouze nové a změněné soubory	Kontroluje pouze nové soubory a soubory, které byly od posledního skenování změněny. To pomáhá zkrátit dobu skenování. Tento režim se vztahuje jak na jednoduché, tak na složené soubory.

Přeskočit soubory, které se kontrolují déle než N s	Omezí dobu trvání kontroly jednoho objektu. Po zadané době aplikace Kaspersky Endpoint Security ukončí kontrolu souboru. To pomáhá zkrátit dobu skenování.
Kontrolovat archivy	Prohledává archivy v následujících formátech: RAR, ARJ, ZIP, CAB, LHA, JAR a ICE.
Kontrolovat distribuční balíčky	Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat kontrolu distribučních balíčků.
Kontrolovat soubory ve formátu aplikací Microsoft Office	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE.
Nerozbalovat velké složené soubory	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu.
Strojové učení a analýza signatur	Metoda strojového učení a analýzy signatur používá databáze aplikace Kaspersky Endpoint Security, které obsahují popisy známých hrozeb a způsoby jejich neutralizace. Ochrana využívající tuto metodu poskytuje minimální přijatelnou úroveň zabezpečení. Na základě doporučení odborníků společnosti Kaspersky je metoda strojového učení a analýzy signatur vždy povolena.
Heuristická analýza	Tato technologie byla vyvinuta za účelem zjišťování hrozeb, které nelze zjistit na základě aktuální verze databází aplikací společnosti Kaspersky. Umožňuje zjišťovat soubory, které mohou být nakaženy neznámým virem nebo novou variantou známého viru. Při kontrole souborů na výskyt škodlivého kódu provede heuristický analyzátor pokyny ve spustitelných souborech. Počet instrukcí, které jsou prováděny heuristickým analyzátorem, závisí na úrovni pro něj určené. Úroveň heuristické analýzy zajišťuje rovnováhu mezi podrobností hledání, zatížením prostředků operačního systému a trváním heuristické analýzy.
Technologie iSwift	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iSwift je vylepšením technologie iChecker pro souborový systém NTFS.
Technologie iChecker	Tato technologie umožňuje zvýšit rychlost kontroly vyloučením určitých souborů z kontroly. Soubory jsou vyloučeny z kontroly pomocí speciálního algoritmu, který zohledňuje datum vydání databází aplikace Kaspersky Total Security, datum poslední kontroly souboru a jakékoli úpravy provedené v nastavení kontroly. Technologie iChecker má svá omezení: Nefunguje u velkých souborů a vztahuje se pouze na soubory se strukturou, kterou aplikace rozpoznává (například EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP a RAR).

Kontrola vyměnitelných jednotek

Aplikace Kaspersky Endpoint Security umožňuje kontrolovat vyměnitelné jednotky připojené k počítači na přítomnost virů a jiného malwaru.

Nastavení úlohy Kontrola vyměnitelných jednotek

Parametr	Popis
Akce při připojení vyměnitelné jednotky	• **Nekontrolovat**. • **Podrobná kontrola** Je-li tato možnost vybrána, po připojení vyměnitelné jednotky aplikace Kaspersky Endpoint Security zkontroluje všechny soubory, které se nachází na vyměnitelné jednotce, včetně souborů ve složených objektech. • **Rychlá kontrola** Je-li tato možnost vybrána, po připojení vyměnitelné jednotky aplikace Kaspersky Endpoint Security zkontroluje pouze soubory v konkrétních formátech, které jsou na infekce nejnáchylnější, a nerozbalí složené objekty.
Maximální velikost vyměnitelné jednotky	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security provede akci, která je vybrána v rozevíracím seznamu **Akce při připojení vyměnitelné jednotky** u vyměnitelných jednotek, jejichž velikost nepřekračuje maximální určenou velikost jednotky. Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security provede akci, která je vybrána v rozevíracím seznamu **Akce při připojení vyměnitelné jednotky** u vyměnitelných jednotek libovolné velikosti.
Zobrazit průběh kontroly	Pokud je toto políčko zaškrtnuto, bude aplikace Kaspersky Endpoint Security zobrazovat průběh kontroly vyměnitelných jednotek v samostatném okně a v okně **Úlohy**. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude aplikace Kaspersky Endpoint Security provádět kontrolu vyměnitelných jednotek na pozadí.
Blokovat zastavení úlohy kontroly	Pokud je políčko zaškrtnuto, tlačítko **Zastavit** v okně **Úlohy** a tlačítko **Zastavit** v okně **Antivirová kontrola** nejsou dostupné v místním rozhraní aplikace Kaspersky Endpoint Security.

Kontrola integrity

Aplikace Kaspersky Endpoint Security kontroluje, zda u souborů aplikace v instalační složce aplikace nedošlo ke změnám nebo poškození. Pokud má například knihovna aplikace nesprávný digitální podpis, je považována za poškozenou. Úloha *Kontrola integrity* je určena ke kontrole souborů aplikací. Úlohu *Kontrola integrity* spusťte, pokud aplikace Kaspersky Endpoint Security zjistila škodlivý objekt, ale neneutralizovala ho.

Úlohu *Kontrola integrity* můžete vytvořit jak ve webové konzole aplikace Kaspersky Security Center 12, tak v konzole pro správu. Tuto úlohu nelze vytvořit v cloudové konzole Kaspersky Security Center.

K porušení integrity aplikace může dojít v následujících případech:

- Škodlivý objekt změnil soubory aplikace Kaspersky Endpoint Security. V takovém případě proveďte postup obnovení aplikace Kaspersky Endpoint Security pomocí nástrojů operačního systému. Po obnovení spusťte úplnou kontrolu počítače a zopakujte kontrolu integrity.
- Platnost digitálního podpisu skončila. V takovém případě aktualizujte aplikaci Kaspersky Endpoint Security.

Nastavení úlohy Kontrola integrity

Parametr	Popis
Plán kontrol	**Ručně**. Režim spuštění, ve kterém můžete kontrolu spustit ručně v době, kdy je to pro

	vás výhodné. **Naplánováno**. V tomto režimu spuštění úlohy kontroly bude aplikace Kaspersky Endpoint Security spouštět úlohu kontroly podle vytvořeného plánu. Pokud je vybrán tento režim spuštění úlohy kontroly, je možné úlohu kontroly spustit i ručně.
Spustit neprovedené úlohy	Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu kontroly, jakmile to bude možné. Úlohu kontroly lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy kontroly. Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security vynechané úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu kontroly.
Spustit pouze v době, kdy je počítač neaktivní	Odložené spuštění úlohy kontroly, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky.
Spustit jako *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Ve výchozím nastavení je úloha kontroly spuštěna pod jménem uživatele, s jehož právy jste zaregistrováni v operačním systému. Pro přístup k instalační složce aplikace mohou být vyžadována zvláštní oprávnění. Můžete zadat uživatele, který má požadovaná práva v nastavení úlohy kontroly, a úlohu kontroly spustit pod účtem tohoto uživatele.

Aktualizace databází a softwarových modulů aplikace

Aktualizace databází a modulů aplikace Kaspersky Endpoint Security zajišťuje maximální ochranu počítače. Nové viry a jiné typy malwaru se objevují po celém světě každý den. Databáze aplikace Kaspersky Endpoint Security obsahují informace o hrozbách a možnostech jejich zneškodnění. Pro rychlou detekci hrozeb je důležité, aby byly databáze a moduly aplikace pravidelně aktualizovány.

Pravidelné aktualizace vyžadují platnou licenci. Pokud nemáte k dispozici žádnou licenci, aktualizaci budete moci provést jen jednou.

Hlavním zdrojem aktualizací pro aplikaci Kaspersky Endpoint Security jsou aktualizační servery společnosti Kaspersky.

Aby bylo možné stáhnout z aktualizačních serverů společnosti Kaspersky balíčky aktualizací, počítač musí být připojený k internetu. Nastavení připojení k internetu je ve výchozím nastavení určováno automaticky. Pokud používáte proxy server, musíte konfigurovat jeho nastavení.

Aktualizace se stahují přes protokol HTTPS. Když není možné aktualizace stahovat přes protokol HTTPS, mohou se také stahovat přes protokol HTTP.

Při provádění aktualizace jsou do počítače staženy a nainstalovány následující objekty:

- Databáze aplikace Kaspersky Endpoint Security. Ochrana počítače je zajišťována pomocí databází, které obsahují podpisy virů a jiných hrozeb a informace o tom, jak je lze zneškodnit. Součásti ochrany tyto informace

používají při hledání a zneškodňování infikovaných souborů v počítači. Databáze jsou neustále aktualizovány záznamy o nových hrozbách a způsobech jejich zneškodnění. Proto je doporučujeme aktualizovat pravidelně.

Kromě databází aplikace Kaspersky Endpoint Security jsou také aktualizovány síťové ovladače, které umožňují součástem aplikace zachytit síťový provoz.

- Moduly aplikace. Kromě databází aplikace Kaspersky Endpoint Security můžete aktualizovat také moduly aplikace. Aktualizace modulů aplikace opravuje zranitelnosti v aplikaci Kaspersky Endpoint Security, přidává nové funkce nebo vylepšuje ty stávající.

Moduly aplikace a databáze v počítači jsou při aktualizaci porovnávány s aktuální verzí ve zdroji aktualizace. Pokud se vaše současné databáze a moduly aplikace liší od příslušných aktuálních verzí, do počítače se nainstalují chybějící části aktualizace.

S aktualizací modulů aplikace lze aktualizovat všechny soubory kontextové nápovědy.

Pokud jsou databáze zastaralé, balíček aktualizace může být velký, což může způsobit dodatečný internetový provoz (až několik desítek MB).

Informace o aktuálním stavu databází aplikace Kaspersky Endpoint Security se zobrazí v části **Aktualizace** v okně **Úlohy**.

Informace o výsledcích aktualizace a všech událostech, k nimž dojde během aktualizace, jsou zaznamenávány do zprávy aplikace Kaspersky Endpoint Security.

Nastavení aktualizace modulů a databází aplikace

Parametr	Popis
Režim spuštění	**Automaticky**. V tomto režimu aplikace Kaspersky Endpoint Security kontroluje zdroj aktualizace nových aktualizačních balíčků v určitých intervalech. Četnost kontrol aktualizačního balíčku se může zvýšit v období virové epidemie a snížit v době, kdy nejsou žádné nové viry. Po zjištění nového aktualizačního balíčku jej aplikace Kaspersky Endpoint Security stáhne a nainstaluje aktualizace do počítače. **Ručně**. Tento režim spuštění úlohy aktualizace umožňuje spustit úlohu aktualizace ručně. **Naplánováno**. V tomto režimu spuštění úlohy aktualizace aplikace Kaspersky Endpoint Security spustí úlohu aktualizace v souladu se zadaným plánem. Je-li vybrán tento režim spuštění úlohy aktualizace, lze úlohu aktualizace aplikace Kaspersky Endpoint Security spustit také ručně.
Spustit neprovedené úlohy	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security spustí neprovedenou úlohu aktualizace, co nejdříve to bude možné. Úlohu aktualizace lze vynechat, například pokud byl počítač vypnut v době spuštění úlohy aktualizace. Není-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nespustí vynechané úlohy aktualizace. Namísto toho spustí další úlohu aktualizace podle aktuálního plánu.
Zdroj aktualizací	*Zdroj aktualizací* je prostředek, který obsahuje aktualizace pro databáze a moduly aplikace Kaspersky Endpoint Security. Zdroje aktualizací zahrnují server aplikace Kaspersky Security Center, aktualizační servery společnosti Kaspersky a síťové nebo místní složky. Výchozí seznam zdrojů aktualizací zahrnuje aplikaci Kaspersky Security Center a aktualizační servery společnosti Kaspersky. Do seznamu můžete přidat další zdroje aktualizací. Jako zdroje aktualizací můžete určit servery HTTP/FTP a sdílené složky.

	Aplikace Kaspersky Endpoint Security nepodporuje aktualizace ze serverů HTTPS, pokud nejde o aktualizační servery společnosti Kaspersky. Pokud je více prostředků vybráno jako zdroje aktualizací, aplikace Kaspersky Endpoint Security se pokusí o postupné připojení ke každému z nich, počínaje od začátku seznamu, a provede úlohu aktualizace získáním aktualizačního balíčku z prvního dostupného zdroje.
Spustit tuto úlohu jako	Ve výchozím nastavení je úloha aktualizace aplikace Kaspersky Endpoint Security spuštěna jménem uživatele, jehož účet byl použit k přihlášení do operačního systému. Aplikace Kaspersky Endpoint Security však může být aktualizována ze zdroje, ke kterému nemá uživatel přístup kvůli nedostatečným oprávněním (například sdílená složka obsahující balíček aktualizace), nebo ze zdroje, u kterého není nakonfigurováno ověření proxy serveru. V nastavení Kaspersky Endpoint Security můžete určit uživatele, který potřebná oprávnění má, a spustit úlohu aktualizace aplikace Kaspersky Endpoint Security v rámci účtu tohoto uživatele.
Stáhnout aktualizace modulů aplikace	Toto zaškrtávací políčko povoluje/zakazuje stažení aktualizací modulu aplikace spolu s aktualizacemi antivirových databází. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security informuje uživatele o dostupných aktualizacích modulu aplikace a zahrne aktualizace modulu aplikace do aktualizačního balíčku během spuštění úlohy aktualizace. Způsob, jakým jsou aktualizace modulu aplikace použity, je určen následujícími nastaveními: • **Instalovat důležité a schválené aktualizace**. Pokud je tato možnost vybrána, když jsou dostupné aktualizace modulu aplikace, aplikace Kaspersky Endpoint Security nainstaluje automaticky důležité aktualizace a všechny ostatní aktualizace modulu aplikace až poté, co bude jejich instalace schválena místně prostřednictvím rozhraní aplikace nebo ze strany služby Kaspersky Security Center. • **Instalovat pouze schválené aktualizace**. Pokud je tato možnost vybrána, když jsou dostupné aktualizace modulu aplikace, aplikace Kaspersky Endpoint Security je nainstaluje až poté, co bude jejich instalace schválena místně prostřednictvím rozhraní aplikace nebo ze strany služby Kaspersky Security Center. Tato možnost je nastavena jako výchozí. Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nebude informovat uživatele o dostupných aktualizacích modulu aplikace a nezahrne aktualizace modulu aplikace do aktualizačního balíčku během spuštění úlohy aktualizace. Pokud aktualizace modulu aplikace vyžadují kontrolu a přijetí podmínek Licenční smlouvy s koncovým uživatelem, aplikace nainstaluje aktualizace po přijetí podmínek Licenční smlouvy s koncovým uživatelem. Ve výchozím nastavení je toto políčko zaškrtnuto.
Zkopírovat aktualizace do složky	Pokud je toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security zkopíruje aktualizační balíček do sdílené složky vybrané pod zaškrtávacím políčkem. Poté budou další počítače ve vaší síti LAN schopné obdržet aktualizační balíček z této sdílené složky. Tím se snižuje internetový provoz, protože aktualizační balíček je stahován pouze jednou. Ve výchozím nastavení je vybrána následující složka: `C:\ProgramData\Kaspersky Lab\KES\Update distribution\`.
Proxy server pro aktualizace	Nastavení proxy serveru pro přístup uživatelů klientských počítačů k internetu za účelem aktualizace modulů a databází aplikace.

(k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security)	Pro automatickou konfiguraci proxy serveru použije aplikace Kaspersky Endpoint Security protokol WPAD (Web Proxy Auto-Discovery Protocol). Pokud nelze IP adresu proxy serveru pomocí tohoto protokolu určit, aplikace Kaspersky Endpoint Security použije adresu proxy serveru zadanou v nastavení prohlížeče Microsoft Internet Explorer.
Nepoužívat proxy server pro adresy vnitřní sítě *(k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security)*	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nepoužije proxy serveru při provádění aktualizace ze sdílené složky.

Příloha 2. Skupiny důvěryhodnosti aplikací

Aplikace Kaspersky Endpoint Security kategorizuje všechny aplikace spouštěné v počítači do skupin důvěryhodnosti. Aplikace jsou kategorizovány do skupin důvěryhodnosti v závislosti na úrovni hrozby, kterou představují pro operační systém.

Skupiny důvěryhodnosti jsou následující:

- **Důvěryhodné**. Tato skupina zahrnuje aplikace, které splňují jednu nebo více následujících podmínek:
  - Aplikace je digitálně podepsána důvěryhodným dodavatelem.
  - Aplikace je zaznamenána v databázi důvěryhodných aplikací služby Kaspersky Security Network.
  - Uživatel umístil aplikaci do skupiny „Důvěryhodné“.

  U těchto aplikací nejsou zakázány žádné operace.
- **Nízké omezení**. Tato skupina zahrnuje aplikace, které splňují následující podmínky:
  - Aplikace není digitálně podepsána důvěryhodným dodavatelem.
  - Aplikace není zaznamenána v databázi důvěryhodných aplikací služby Kaspersky Security Network.
  - Uživatel umístil aplikaci do skupiny „Nízké omezení“.

  Na takovéto aplikace se vztahují minimální omezení přístupu k prostředkům operačního systému.
- **Vysoké omezení**. Tato skupina zahrnuje aplikace, které splňují následující podmínky:
  - Aplikace není digitálně podepsána důvěryhodným dodavatelem.
  - Aplikace není zaznamenána v databázi důvěryhodných aplikací služby Kaspersky Security Network.
  - Uživatel umístil aplikaci do skupiny „Vysoké omezení“.

Na takovéto aplikace se vztahují výrazná omezení přístupu k prostředkům operačního systému.

- **Nedůvěryhodné**. Tato skupina zahrnuje aplikace, které splňují následující podmínky:
  - Aplikace není digitálně podepsána důvěryhodným dodavatelem.
  - Aplikace není zaznamenána v databázi důvěryhodných aplikací služby Kaspersky Security Network.
  - Uživatel umístil aplikaci do skupiny „Nedůvěryhodné“.

  U těchto aplikací jsou všechny operace blokovány.

Příloha 3. Přípony souborů pro rychlou kontrolu vyměnitelných jednotek

com – spustitelný soubor aplikace, který není větší než 64 kB

exe – spustitelný soubor nebo samorozbalovací archiv

sys – soubor systému Microsoft Windows

prg – programový text pro programy dBase™, Clipper nebo Microsoft Visual FoxPro® nebo WAVmaker

bin – binární soubor

bat – dávkový soubor

cmd – příkazový soubor pro systém Microsoft Windows NT (je podobný souboru bat pro systém DOS), OS/2

dpl – komprimovaná knihovna Borland Delphi

dll – dynamická knihovna

scr – úvodní obrazovka systému Microsoft Windows

cpl – modul ovládacího panelu Microsoft Windows

ocx – objekt Microsoft OLE (technologie Object Linking and Embedding)

tsp – program běžící v režimu mezičasu

drv – ovladače zařízení

vxd – ovladač virtuálního zařízení systému Microsoft Windows

pif – soubor PIF

lnk – soubor odkazu systému Microsoft Windows

reg – soubor klíče registru systému Microsoft Windows

ini – konfigurační soubor, který obsahuje konfigurační data pro systémy Microsoft Windows, Windows NT a některé aplikace

cla – třída Java

vbs – skript jazyka Visual Basic®

vbe – rozšíření systému BIOS pro video

js, jse – zdrojový text JavaScript

htm – hypertextový dokument

htt – hlavička hypertextu systému Microsoft Windows

hta – hypertextový program pro aplikaci Microsoft Internet Explorer®

asp – skript Active Server Pages

chm – zkompilovaný soubor HTML

pht – soubor HTML s integrovanými skripty PHP

php – skript integrovaný do souborů HTML

wsh – soubor prostředí Microsoft Windows Script Host

wsf – skript systému Microsoft Windows

the – soubor tapety pro plochu systému Microsoft Windows 95

hlp – soubor nápovědy Win Help

eml – e-mailová zpráva aplikace Microsoft Outlook Express

nws – nová e-mailová zpráva aplikace Microsoft Outlook Express

msg – e-mailová zpráva Microsoft Mail

plg – e-mailová zpráva

mbx – uložená e-mailová zpráva aplikace Microsoft Office Outlook

doc* – dokumenty aplikace Microsoft Office Word, například: doc pro dokumenty aplikace Microsoft Office Word, docx pro dokumenty aplikace Microsoft Office Word 2007 s podporou jazyka XML a docm pro dokumenty aplikace Microsoft Office Word 2007 s podporou maker

dot* – šablony dokumentů aplikace Microsoft Office Word, například: dot pro šablony dokumentů aplikace Microsoft Office Word, dotx pro šablony dokumentů aplikace Microsoft Office Word 2007, dotm pro šablony dokumentů aplikace Microsoft Office Word 2007 s podporou maker

fpm – databázový program, spouštěcí program Microsoft Visual FoxPro

rtf – dokument formátu Rich Text Format

shs – fragment obslužné rutiny objektu Windows Shell Scrap

dwg – databáze výkresů AutoCAD®

msi – balíček instalační služby systému Microsoft Windows

otm – projekt VBA pro aplikaci Microsoft Office Outlook

pdf – dokument aplikace Adobe Acrobat

swf – objekt balíčku Shockwave® Flash

jpg, jpeg – formát komprimovaného obrázku

emf – soubor Enhanced Metafile Format;

ico – soubor ikon objektů

ov? – spustitelné soubory aplikace Microsoft Office Word

xl* – dokumenty a soubory aplikace Microsoft Office Excel, například: xla, rozšíření pro aplikaci Microsoft Office Excel, xlc pro diagramy, xlt pro šablony dokumentů, xlsx pro sešity aplikace Microsoft Office Excel 2007, xltm pro sešity aplikace Microsoft Office Excel 2007 s podporou maker, xlsb pro sešity aplikace Microsoft Office Excel 2007 v binárním formátu (ne XML), xltx pro šablony aplikace Microsoft Office Excel 2007, xlsm pro šablony aplikace Microsoft Office Excel 2007 s podporou maker a xlam pro doplňky aplikace Microsoft Office Excel 2007 s podporou maker

pp* – dokumenty a soubory aplikace Microsoft Office PowerPoint®, například: pps pro snímky aplikace Microsoft Office PowerPoint, ppt pro prezentace, pptx pro prezentace aplikace Microsoft Office PowerPoint 2007, pptm pro prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker, potx pro šablony prezentace aplikace Microsoft Office PowerPoint 2007, potm pro šablony prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker, ppsx pro prezentace aplikace Microsoft Office PowerPoint 2007, ppsm pro prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker a ppam pro doplňky aplikace Microsoft Office PowerPoint 2007 s podporou maker

md* – dokumenty a soubory aplikace Microsoft Office Access®, například: mda pro pracovní skupiny Microsoft Office Access a mdb pro databáze

sldx – snímek aplikace Microsoft PowerPoint 2007

sldm – snímek aplikace Microsoft PowerPoint 2007 s podporou maker

thmx – motiv sady Microsoft Office 2007

Příloha 4. Typy souborů pro filtr příloh Ochrana před hrozbami v poště

Berte na vědomí, že skutečný formát souboru nemusí odpovídat příponě souboru.

Pokud jste povolili filtrování e-mailových příloh, součást Ochrana před hrozbami v poště může přejmenovat nebo odstranit soubory s následujícími příponami:

com – spustitelný soubor aplikace, který není větší než 64 kB

exe – spustitelný soubor nebo samorozbalovací archiv

sys – soubor systému Microsoft Windows

prg – programový text pro programy dBase™, Clipper nebo Microsoft Visual FoxPro® nebo WAVmaker

bin – binární soubor

bat – dávkový soubor

cmd – příkazový soubor pro systém Microsoft Windows NT (je podobný souboru bat pro systém DOS), OS/2

dpl – komprimovaná knihovna Borland Delphi

dll – dynamická knihovna

scr – úvodní obrazovka systému Microsoft Windows

cpl – modul ovládacího panelu Microsoft Windows

ocx – objekt Microsoft OLE (technologie Object Linking and Embedding)

tsp – program běžící v režimu mezičasu

drv – ovladače zařízení

vxd – ovladač virtuálního zařízení systému Microsoft Windows

pif – soubor PIF

lnk – soubor odkazu systému Microsoft Windows

reg – soubor klíče registru systému Microsoft Windows

ini – konfigurační soubor, který obsahuje konfigurační data pro systémy Microsoft Windows, Windows NT a některé aplikace

cla – třída Java

vbs – skript jazyka Visual Basic®

vbe – rozšíření systému BIOS pro video

js, jse – zdrojový text JavaScript

htm – hypertextový dokument

htt – hlavička hypertextu systému Microsoft Windows

hta – hypertextový program pro aplikaci Microsoft Internet Explorer®

asp – skript Active Server Pages

chm – zkompilovaný soubor HTML

pht – soubor HTML s integrovanými skripty PHP

php – skript integrovaný do souborů HTML

wsh – soubor prostředí Microsoft Windows Script Host

wsf – skript systému Microsoft Windows

the – soubor tapety pro plochu systému Microsoft Windows 95

hlp – soubor nápovědy Win Help

eml – e-mailová zpráva aplikace Microsoft Outlook Express

nws – nová e-mailová zpráva aplikace Microsoft Outlook Express

msg – e-mailová zpráva Microsoft Mail

plg – e-mailová zpráva

mbx – uložená e-mailová zpráva aplikace Microsoft Office Outlook

doc* – dokumenty aplikace Microsoft Office Word, například: doc pro dokumenty aplikace Microsoft Office Word, docx pro dokumenty aplikace Microsoft Office Word 2007 s podporou jazyka XML a docm pro dokumenty aplikace Microsoft Office Word 2007 s podporou maker

dot* – šablony dokumentů aplikace Microsoft Office Word, například: dot pro šablony dokumentů aplikace Microsoft Office Word, dotx pro šablony dokumentů aplikace Microsoft Office Word 2007, dotm pro šablony dokumentů aplikace Microsoft Office Word 2007 s podporou maker

fpm – databázový program, spouštěcí program Microsoft Visual FoxPro

rtf – dokument formátu Rich Text Format

shs – fragment obslužné rutiny objektu Windows Shell Scrap

dwg – databáze výkresů AutoCAD®

msi – balíček instalační služby systému Microsoft Windows

otm – projekt VBA pro aplikaci Microsoft Office Outlook

pdf – dokument aplikace Adobe Acrobat

swf – objekt balíčku Shockwave® Flash

jpg, jpeg – formát komprimovaného obrázku

emf – soubor Enhanced Metafile Format;

ico – soubor ikon objektů

ov? – spustitelné soubory aplikace Microsoft Office Word

xl* – dokumenty a soubory aplikace Microsoft Office Excel, například: xla, rozšíření pro aplikaci Microsoft Office Excel, xlc pro diagramy, xlt pro šablony dokumentů, xlsx pro sešity aplikace Microsoft Office Excel 2007, xltm pro sešity aplikace Microsoft Office Excel 2007 s podporou maker, xlsb pro sešity aplikace Microsoft Office Excel 2007 v binárním formátu (ne XML), xltx pro šablony aplikace Microsoft Office Excel 2007, xlsm pro šablony aplikace Microsoft Office Excel 2007 s podporou maker a xlam pro doplňky aplikace Microsoft Office Excel 2007 s podporou maker

pp* – dokumenty a soubory aplikace Microsoft Office PowerPoint®, například: pps pro snímky aplikace Microsoft Office PowerPoint, ppt pro prezentace, pptx pro prezentace aplikace Microsoft Office PowerPoint 2007, pptm pro prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker, potx pro šablony prezentace aplikace Microsoft Office PowerPoint 2007, potm pro šablony prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker, ppsx pro prezentace aplikace Microsoft Office PowerPoint 2007, ppsm pro prezentace aplikace Microsoft Office PowerPoint 2007 s podporou maker a ppam pro doplňky aplikace Microsoft Office PowerPoint 2007 s podporou maker

md* – dokumenty a soubory aplikace Microsoft Office Access®, například: mda pro pracovní skupiny Microsoft Office Access a mdb pro databáze

sldx – snímek aplikace Microsoft PowerPoint 2007

sldm – snímek aplikace Microsoft PowerPoint 2007 s podporou maker

thmx – motiv sady Microsoft Office 2007

Příloha 5. Nastavení sítě pro interakci s externími službami

Aplikace Kaspersky Endpoint Security používá pro interakci s externími službami následující nastavení sítě.

Nastavení sítě

Adresa	Popis
`Activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokol: `HTTPS` Port: `443`	Aktivace aplikace

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
	Aktualizace databází a modulů aplikace

`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Protokol: `HTTPS`
Port: `443`	

`downloads.upd.kaspersky.com` Protokol: `HTTPS` Port: `443`	• Aktualizace databází a modulů aplikace • Kontroluje, zda jsou servery Kaspersky přístupné. Pokud není možný přístup k serverům pomocí systémových DNS není možný, aplikace použije veřejné DNS. To je nutné k zajištění aktualizací antivirových databází a zachování úrovně zabezpečení počítače. Aplikace Kaspersky Endpoint Security používá následující seznam veřejných serverů DNS v následujícím pořadí: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).

	Žádosti vysílané aplikací mohou obsahovat adresy domén a veřejné IP adresy uživatele, protože aplikace navazuje se serverem DNS připojení TCP/UDP. Tyto údaje jsou nutné například k ověření certifikátu webového prostředku při používání HTTPS. Pokud aplikace Kaspersky Endpoint Security používá veřejný server DNS, zpracování údajů se řídí zásadami osobních údajů příslušné služby. Jestliže si nepřejete, aby aplikace Kaspersky Endpoint Security používala veřejný server DNS, požádejte technickou podporu o privátní opravu.
`touch.kaspersky.com` Protokol: `HTTP`	• Příjem důvěryhodného času pro kontrolu doby platnosti certifikátu (připojení TLS). • Upozornění na odepření přístupu k webovému prostředku v prohlížeči (Ochrana před webovými hrozbami a Kontrola webu)

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
	Aktualizace databází a modulů aplikace

`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protokol: `HTTP`
Port: `80`	

`ds.kaspersky.com` Protokol: `HTTPS` Port: `443`	Používání služby Kaspersky Security Network

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protokol: `Any`
Port: `443`, `1443`
	Používání služby Kaspersky Security Network

`click.kaspersky.com`
`redirect.kaspersky.com`
Protokol: `HTTPS`
	Postupujte podle odkazů z rozhraní

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokol: `HTTP`
Port: `80`
	Infrastruktura veřejného klíče (PKI)

Příloha 6. Události aplikace v protokolu událostí systému Windows

V protokolu událostí systému Windows jsou zaznamenávány informace o provozu každé součásti aplikace Kaspersky Endpoint Security, událostech šifrování dat, provedení každé úlohy kontroly, úlohy aktualizace, úlohy kontroly integrity a také o celkovém fungování aplikace.

Audit systému

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
201	Porušení licenční smlouvy s koncovým uživatelem	✓
203	Licence téměř vypršela	–
204	Platnost licence brzy vyprší	–
206	Databáze chybí nebo jsou poškozené	–
207	Databáze jsou extrémně zastaralé	–
208	Databáze jsou zastaralé	–
209	Automatické spouštění aplikace je zakázáno	–
210	Automatické aktualizace jsou zakázány	–
211	Sebeobrana je zakázána	–
212	Úlohu nelze spustit	–
213	Sebeobrana blokuje operace s prostředky aplikace	–
214	Jsou zakázány součásti ochrany	–
215	Počítač běží v nouzovém režimu	–
216	Existují nezpracované soubory	–
217	Vymazání zprávy	✓
218	Změna nastavení aplikace	✓
219	Použití zásad skupiny	✓
220	Zásada skupiny je zakázána	–
221	Úloha byla spuštěna	–
222	Úloha byla zastavena	–
223	Úloha byla dokončena	–
224	Chcete-li aktualizaci dokončit, restartujte aplikaci	–
225	Je nutné restartovat počítač	✓
226	Licence umožňuje použití součástí, které nebyly nainstalovány	–
227	Nainstalované součásti odpovídají licenci	–
229	Chyba aktivace	✓
230	Nesprávný rezervní aktivační kód	–
231	Bylo zjištěno aktivní ohrožení a je nutné spustit pokročilou dezinfekci	–
232	Pokročilá dezinfekce byla spuštěna	–
233	Pokročilá dezinfekce byla dokončena	–
235	Spuštění aplikace	✓
236	Zastavení aplikace	✓
237	Během předchozí relace došlo k pádu aplikace	✓

240	Platnost licence brzy vyprší	✓
238	Změna nastavení předplatného	✓
239	Obnovení předplatného	✓
335	Obnovení objektu ze zálohy	✓
336	Objekt nelze obnovit ze zálohy	✓
245	Zpracování některých funkcí OS je zakázáno	✓
250	Ukončení šifrovaného připojení	✓
708	Nastavení úlohy bylo úspěšně použito	–
335	Obnovení objektu ze zálohy	✓
2000	Zadejte uživatelské jméno a heslo	–
2001	Byla zjištěna podezřelá aktivita v síti	–
2020	Účast ve službě KSN je povolena	–
2021	Účast ve službě KSN je zakázána	–
2022	Servery KSN jsou k dispozici	–
2023	Servery KSN nejsou k dispozici	–
2024	Aplikace funguje a zpracovává data podle platných zákonů a využívá příslušnou infrastrukturu	✓
227	Všechny součásti aplikace, které jsou definovány licencí, byly nainstalovány a spuštěny v normálním režimu	–

Detekce chování

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–
307	Objekt byl odstraněn	–
308	Byla vytvořena záložní kopie objektu	–
311	Nelze vytvořit záložní kopii	–
313	Nelze odstranit	–
323	Objekt bude odstraněn při restartu	–
329	Objekt byl přejmenován	–
331	Blokováno	–
452	Proces byl ukončen	–
453	Proces nelze ukončit	–
455	Vracení bylo dokončeno	–
458	Hodnota registru byla obnovena	–
459	Hodnota registru byla odstraněna	–
453	Spuštění souboru/kódu bylo blokováno	–

Prevence zneužití

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
302	Zjištění škodlivého objektu	–
331	Blokováno	–
455	Vracení bylo dokončeno	–
323	Objekt bude odstraněn při restartu	–
307	Objekt byl odstraněn	–
329	Objekt byl přejmenován	–
457	Soubor byl obnoven	–
458	Hodnota registru byla obnovena	–
459	Hodnota registru byla odstraněna	–

Prevence narušení hostitele

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
301	Objekt byl zpracován	–
302	Zjištění škodlivého objektu	–
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–
306	Objekt byl dezinfikován	–
307	Objekt byl odstraněn	–
308	Byla vytvořena záložní kopie objektu	–
310	Nelze vytvořit záložní kopii	–
312	Dezinfekce není možná	–
313	Nelze odstranit	–
314	Objekt nebyl zpracován	–
315	Objekt byl přeskočen	–
317	Chyba zpracování	✓
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
320	Objekt byl zašifrován	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
323	Objekt bude odstraněn při restartu	–
324	Objekt bude dezinfikován při restartu	–
327	Přepsáno kopií, která byla dříve dezinfikována	–
332	Informace o zjištěném objektu	–
335	Obnovení objektu ze zálohy	–
336	Objekt nelze obnovit ze zálohy	✓
340	Objekt je na seznamu povolených objektů privátní KSN	✓
401	Aplikace byla umístěna do skupiny důvěryhodných	–
402	Aplikace byla umístěna do skupiny s omezením	–
403	Byla spuštěna součást Prevence narušení hostitele	–
452	Proces byl ukončen	–
453	Proces nelze ukončit	–

Ochrana před souborovými hrozbami

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
302	Zjištění škodlivého objektu	✓
317	Chyba zpracování	✓
336	Objekt nelze obnovit ze zálohy	✓
340	Objekt je na seznamu povolených objektů privátní KSN	✓
301	Objekt byl zpracován	–
306	Objekt byl dezinfikován	–
307	Objekt byl odstraněn	–
308	Byla vytvořena záložní kopie objektu	–
310	Nelze vytvořit záložní kopii	–
312	Dezinfekce není možná	–
313	Nelze odstranit	–
314	Objekt nebyl zpracován	–
315	Objekt byl přeskočen	–
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
320	Objekt byl zašifrován	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
323	Objekt bude odstraněn při restartu	–
324	Objekt bude dezinfikován při restartu	–
325	Přepsáno kopií, která byla dříve dezinfikována	–
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–
329	Objekt byl přejmenován	–
335	Obnovení objektu ze zálohy	–
452	Proces byl ukončen	–
453	Proces nelze ukončit	–
332	Informace o zjištěném objektu	–

Ochrana před webovými hrozbami

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
301	Objekt byl zpracován	–
302	Zjištění škodlivého objektu	✓
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–
317	Chyba zpracování	✓
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
329	Objekt byl přejmenován	–
362	Zablokování nebezpečného odkazu	✓
1201	Zjištění dříve otevřeného nebezpečného odkazu	✓
1211	Zjištění dříve otevřeného škodlivého odkazu	✓
363	Otevření nebezpečného odkazu	✓
341	Stahování objektu bylo zablokováno	–
370	Odkaz je na seznamu povolených odkazů privátní KSN	✓
370	Objekt je na seznamu povolených objektů privátní KSN	✓
332	Informace o zjištěném objektu	–

Ochrana před hrozbami v poště

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
301	Objekt byl zpracován	–
306	Objekt byl dezinfikován	–
302	Zjištění škodlivého objektu	✓
317	Chyba zpracování	✓
340	Objekt je na seznamu povolených objektů privátní KSN	✓
307	Objekt byl odstraněn	–
308	Byla vytvořena záložní kopie objektu	–
312	Dezinfekce není možná	–
314	Objekt nebyl zpracován	–
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
329	Objekt byl přejmenován	–
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače	–
332	Informace o zjištěném objektu	–

Brána firewall

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
601	Síťová aktivita povolena	–
602	Síťová aktivita blokována	–

Ochrana před síťovými hrozbami

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
651	Byl zjištěn síťový útok	–

Ochrana před útoky BadUSB

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
2050	Klávesnice autorizována	–
2051	Klávesnice není autorizována	✓
2052	Chyba autorizace klávesnice	✓

Ochrana AMSI

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
301	Objekt byl zpracován	–
302	Zjištění škodlivého objektu	✓
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–
314	Objekt nebyl zpracován	–
315	Objekt byl přeskočen	–
317	Chyba zpracování	✓
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
320	Objekt byl zašifrován	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
1512	Výsledek kontroly objektu byl odeslán do aplikace třetí strany	–
329	Objekt byl přejmenován	–
332	Informace o zjištěném objektu	–
340	Objekt je na seznamu povolených objektů privátní KSN	✓
2200	Zablokování žádosti AMSI	✓

Kontrola aplikací

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
701	Spuštění aplikace je povoleno	–
702	Spuštění aplikace je zakázáno	–
703	Spuštění aplikace je v testovacím režimu zakázáno	–
704	Spuštění aplikace je v testovacím režimu povoleno	–
707	Chyba v nastavení úlohy. Nastavení úlohy není použito	–
710	Zakázaný proces byl spuštěn před spuštěním aplikace Kaspersky Endpoint Security pro systém Windows	–
708	Nastavení úlohy bylo úspěšně použito	–

Kontrola zařízení

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
801	Operace se zařízením je povolena	–
802	Operace se zařízením je zakázána	–
803	Aktivace dočasného přístupu k zařízení	✓
808	Byla provedena operace se souborem	–
809	Síťové připojení blokováno	–

Kontrola webu

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
751	Přístup povolen	–
752	Přístup blokován	–
753	Varování před nežádoucím obsahem	–
754	Po varování bylo přistoupeno k nežádoucímu obsahu	–
751	Otevřena povolená stránka	–

Adaptivní kontrola anomálií

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
501	Stížnost na zablokovanou aktivitu aplikace	–
2201	Akce procesu byla přeskočena	–
2200	Akce procesu blokována	✓

Šifrování dat

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
904	Chyba při používání pravidel šifrování/dešifrování souborů	✓
912	Chyba při šifrování/dešifrování souboru	✓
1305	Chyba při šifrování/dešifrování zařízení	✓
931	Chyba při vytváření šifrovaného balíčku	✓
951	Chyba při povolování mobilního režimu	✓
953	Chyba při zakazování mobilního režimu	✓
1311	Načtení šifrovacího modulu se nezdařilo	✓
1340	Úloha správy účtů agenta ověřování skončila chybou	✓
1312	Zásady nelze použít	✓
1342	Aktualizace FDE se nezdařila	✓
1343	Vrácení aktualizace FDE bylo úspěšné	✓
1345	Instalace nebo upgrade ovladačů Kaspersky Disk Encryption v bitové kopii WinRE se nezdařila	✓
1346	Odinstalace ovladačů Kaspersky Disk Encryption z bitové kopie WinRE se nezdařila	✓
1370	Změna klíče pro obnovení nástroje BitLocker	✓
901	Bylo zahájeno používání pravidel šifrování/dešifrování souborů	–
902	Bylo dokončeno používání pravidel šifrování/dešifrování souborů	–
903	Bylo přerušeno používání pravidel šifrování/dešifrování souborů	–
905	Bylo obnoveno používání pravidel šifrování/dešifrování souborů	–
910	Bylo spuštěno šifrování/dešifrování souboru	–
911	Bylo dokončeno šifrování/dešifrování souboru	–
913	Soubor nebyl zašifrován, protože se jedná o výjimku	–
914	Bylo přerušeno šifrování/dešifrování souboru	–
1301	Bylo spuštěno šifrování/dešifrování zařízení	–
1302	Bylo dokončeno šifrování/dešifrování zařízení	–
1307	Zařízení není šifrováno	–
1303	Bylo přerušeno šifrování/dešifrování zařízení	–
1304	Bylo obnoveno šifrování/dešifrování zařízení	–
1309	Proces šifrování/dešifrování disku byl přepnut do pasivního režimu	–
1308	Proces šifrování/dešifrování zařízení byl přepnut do aktivního režimu	–
1306	Uživatel se vyjádřil nesouhlas se zásadami šifrování	–
940	Zablokování přístupu k souborům	✓
950	Mobilní režim povolen	–

952	Mobilní režim zakázán	–
1330	Byl vytvořen nový účet ověřovacího agenta	–
1337	Účet nebyl přidán. Tento účet již existuje	–
1338	Účet nebyl změněn. Tento účet neexistuje	–
1339	Účet nebyl odstraněn. Tento účet neexistuje	–
1331	Účet ověřovacího agenta byl odstraněn	–
1332	Heslo účtu ověřovacího agenta bylo změněno	–
1334	Neúspěšný pokus o přihlášení ověřovacího agenta	–
1333	Úspěšné přihlášení ověřovacího agenta	–
1335	Přístup k pevnému disku postupem vyžadujícím přístup k šifrovaným zařízením	–
1336	Neúspěšný pokus o přístup k pevnému disku postupem vyžadujícím přístup k šifrovaným zařízením	–
1310	Šifrovací modul načten	–
1344	Vrácení upgradu funkce Úplné šifrování disku bylo dokončeno s chybou	✓
1341	Aktualizace FDE byla úspěšná	✓
1332	Heslo účtu ověřovacího agenta bylo změněno	–

Endpoint Sensor

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
2100	Server platformy Kaspersky Anti Targeted Attack není k dispozici	–
2105	Zablokování spuštění aplikace	✓
2106	Zablokování otevírání dokumentu	✓
2104	Zpracovávají se úlohy ze serveru platformy Kaspersky Anti Targeted Attack	–
2103	Zpracování úloh ze serveru platformy Kaspersky Anti Targeted Attack je neaktivní	–
2101	Senzory koncového bodu připojeny k serveru	–
2102	Bylo obnoveno připojení k serveru platformy Kaspersky Anti Targeted Attack	–
2112	Ukončení všech procesů spuštěných z bitové kopie souboru nebo streamu	✓
2113	Spuštění aplikace	✓
2111	Odstranění souboru nebo streamu správcem serveru Kaspersky Anti Targeted Attack Platform	✓
2110	Obnovení souboru z karantény na serveru Kaspersky Anti Targeted Attack Platform správcem	✓
2109	Umístění souboru do karantény na serveru Kaspersky Anti Targeted Attack Platform správcem	✓
2107	Zablokování síťové aktivity všech aplikací třetích stran	✓
2108	Odblokování síťové aktivity všech aplikací třetích stran	✓

Kontrola počítače

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
302	Zjištění škodlivého objektu	✓
335	Obnovení objektu ze zálohy	✓
336	Objekt nelze obnovit ze zálohy	✓
340	Objekt je na seznamu povolených objektů privátní KSN	✓
301	Objekt byl zpracován	–
329	Objekt byl přejmenován	–
306	Objekt byl dezinfikován	–
307	Objekt byl odstraněn	–
308	Byla vytvořena záložní kopie objektu	–
310	Nelze vytvořit záložní kopii	–
312	Dezinfekce není možná	–
313	Nelze odstranit	–
314	Objekt nebyl zpracován	–
315	Objekt byl přeskočen	–
317	Chyba zpracování	–
318	Byl zjištěn archiv	–
319	Byly zjištěny komprimované soubory	–
320	Objekt byl zašifrován	–
321	Objekt je poškozen	–
322	Byl zjištěn archiv chráněný heslem	–
323	Objekt bude odstraněn při restartu	–
324	Objekt bude dezinfikován při restartu	–
327	Přepsáno kopií, která byla dříve dezinfikována	–
303	Byl zjištěn legitimní software, který lze použít zločinným způsobem k poškození počítače nebo osobních dat	–

Kontrola integrity

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
2002	Kontrola podpisu systémového modulu se nezdařila	–

Aktualizace databáze

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
101	Vyskytla se vnitřní chyba	✓
1001	Byl vybrán zdroj aktualizace	–
1002	Byl vybrán proxy server	–
1003	Stažení souboru	–
1004	Soubor stažen	–
1005	Soubor nainstalován	–
1006	Soubor aktualizován	–
1007	Soubor vrácen zpět kvůli chybě aktualizace	–
1008	Aktualizace souborů	–
1009	Distribuce aktualizací	–
1010	Vrácení souborů zpět	–
1011	Chyba při aktualizaci součásti	–
1012	Chyba při distribuci aktualizací součástí	–
1013	Vytváření seznamu souborů ke stažení	–
1014	Chyba místní aktualizace	–
1016	Operace zrušena uživatelem	–
1017	Nelze spustit dvě úlohy současně	–
1018	Chyba při ověřování databází a modulů aplikací	–
1019	Chyba při interakci s aplikací Kaspersky Security Center	–
1020	Žádné dostupné aktualizace	–
1021	Ne všechny součásti byly aktualizovány	–
1022	Distribuce aktualizace byla úspěšně dokončena	–
1023	Aktualizace byla úspěšně dokončena, distribuce aktualizace se nezdařila	–
2153	Instalace opravy se nezdařila	–
2156	Vrácení opravy se nezdařilo	–
2150	Stahování oprav	–
2151	Instalace oprav	–
2152	Oprava nainstalována	–
2154	Vracení opravy	–
2155	Oprava vrácena	–

Vymazat data

Kódy událostí

ID události	Popis	Ve výchozím nastavení povoleno
223	Úloha byla dokončena	–
221	Úloha byla spuštěna	–
222	Úloha byla zastavena	–
2252	Objekt nelze odstranit	–
2253	Vymazat statistiky úlohy	–
2251	Objekt byl odstraněn	–

Informace o kódu třetích stran

Informace o kódu třetích stran je obsažená v souboru nazvaném legal_notices.txt a uloženém v instalační složce aplikace.

Informace o ochranných známkách

Registrované obchodní značky a servisní značky jsou vlastnictvím příslušných vlastníků.

Adobe, Acrobat, Flash, Reader a Shockwave jsou registrované ochranné známky společnosti Adobe Systems Incorporated v USA a/nebo dalších zemích.

Apple, FireWire, iTunes a Safari jsou ochranné známky společnosti Apple Inc. zaregistrované v USA a dalších zemích.

AutoCAD je ochranná známka nebo registrovaná ochranná známka společnosti Autodesk, Inc. a/nebo jejích dceřiných společností/poboček v USA a/nebo dalších zemích.

Slovo, značku a loga Bluetooth vlastní společnost Bluetooth SIG, Inc.

Borland je ochranná známka nebo registrovaná ochranná známka společnosti Borland Software Corporation.

Android a Google Chrome jsou ochranné známky společnosti Google, Inc.

Citrix a Citrix Provisioning Services a XenDesktop jsou ochranné známky společnosti Citrix Systems, Inc. a/nebo jedné či více jejích dceřiných společností a mohou být zaregistrovány patentovým úřadem USA a v dalších zemích.

Dell je ochranná známka společnosti Dell, Inc. nebo jejích dceřiných společností.

dBase je ochranná známka společnosti dataBased Intelligence, Inc.

EMC je ochranná známka nebo registrovaná ochranná známka společnosti EMC Corporation v USA a/nebo dalších zemích.

Radmin je registrovaná ochranná známka společnosti Famatech.

IBM je ochranná známky společnosti International Business Machines Corporation zaregistrovaná v mnoha jurisdikcích po celém světě.

ICQ je ochranná známka a/nebo značka služby společnosti ICQ LLC.

Intel je ochranná známka společnosti Intel Corporation v USA a/nebo dalších zemích.

IOS je registrovaná ochranná známka společnosti Cisco Systems, Inc. a/nebo jejích dceřiných společností v USA a dalších zemích.

Lenovo a ThinkPad jsou ochranné známky společnosti Lenovo v USA a/nebo dalších zemích.

Linux je registrovaná ochranná známka Linuse Torvaldse v USA a dalších zemích.

Logitech je registrovaná ochranná známka nebo ochranná známka společnosti Logitech v USA a/nebo dalších zemích.

LogMeIn Pro a Remotely Anywhere jsou ochranné známky společnosti LogMeIn, Inc.

Mail.ru je registrovaná ochranná známka společnosti Mail.Ru, LLC.

McAfee je ochranná známka nebo registrovaná ochranná známka společnosti McAfee, Inc. v USA a dalších zemích.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface a Hyper-V jsou registrované ochranné známky společnosti Microsoft Corporation v USA a dalších zemích.

Mozilla, Firefox a Thunderbird jsou ochranné známky společnosti Mozilla Foundation.

Java a JavaScript jsou registrované ochranné známky společnosti Oracle a/nebo jejích dceřiných společností.

VERISIGN je registrovaná ochranná známka v USA a dalších zemích nebo neregistrovaná ochranná známka společnosti VeriSign, Inc. a jejích dceřiných společností.

VMware a VMware ESXi jsou registrované ochranné známky společnosti VMware, Inc. V USA a/nebo dalších jurisdikcích.

Thawte je ochranná známka nebo registrovaná ochranná známka společnosti Symantec Corporation nebo jejích dceřiných společností v USA a dalších zemích.

SAMSUNG je ochranná známka společnosti SAMSUNG v USA a dalších zemích.