Kaspersky Endpoint Security 14.0 pro systém Windows

© 2026 AO Kaspersky Lab

Obsah

- Nápověda k aplikaci Kaspersky Endpoint Security pro systém Windows
  - Co je nového
  - Často kladené dotazy
- Kaspersky Endpoint Security pro systém Windows
  - Režimy aplikace: Standardní, EDR Agent, Light Agent
  - Distribuční sada
  - Hardwarové a softwarové požadavky
  - Porovnání dostupných funkcí aplikace v závislosti na typu operačního systému
  - Porovnání funkcí aplikace v závislosti na nástrojích správy
  - Kompatibilita s jinými aplikacemi
- Instalace a odebrání aplikace
  - Nasazení prostřednictvím aplikace Kaspersky Security Center
    - Standardní instalace aplikace
    - Vytvoření instalačního balíčku
    - Aktualizace databází v instalačním balíčku
    - Vytvoření úlohy vzdálené instalace
  - Místní instalace aplikace pomocí průvodce
  - Vzdálená instalace aplikace pomocí aplikace System Center Configuration Manager
  - Popis nastavení instalace souboru setup.ini
  - Změnit součásti aplikace
  - Upgradování předchozí verze aplikace
    - Upgrade aplikace bez restartování
    - Aktualizace SMU aplikace
  - Odebrání aplikace
- Poskytování licence na aplikaci
  - O licenční smlouvě s koncovým uživatelem (EULA)
  - O licenci
  - O licenčním certifikátu
  - O předplatném
  - O licenčním klíči
  - O aktivačním kódu
  - O souboru klíče
  - Porovnání fungování aplikací v závislosti na typu licence pro pracovní stanice
  - Porovnání fungování aplikací v závislosti na typu licence pro servery
  - Aktivace aplikace
  - Odebírání licenčního klíče
  - Zobrazení informací o licenci
  - Zakoupení licence
  - Obnovení předplatného
- Poskytování údajů
  - Poskytování údajů na základě licenční smlouvy s koncovým uživatelem
  - Poskytování dat při používání služby Kaspersky Security Network
  - Poskytování dat při používání řešení Detection and Response
    - Kaspersky Endpoint Detection and Response
    - Kaspersky Sandbox
    - Kaspersky Endpoint Detection and Response Expert (on-premise)
    - Kaspersky Network Detection and Response (KATA)
    - Integrace s platformou Kaspersky Unified Monitoring and Analysis Platform (KUMA)
  - Soulad s právními předpisy Evropské unie (GDPR)
- Začínáme
  - O modulu plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows
  - Zvláštní požadavky na práci s různými verzemi modulů plug-in administrace
  - Zvláštní úvahy při používání šifrovaných protokolů pro interakci s externími službami
  - Rozhraní aplikace
    - Ikona Aplikace v oznamovací oblasti hlavního panelu
    - Zjednodušené rozhraní aplikace
    - Konfigurace zobrazení rozhraní aplikace

- Příprava aplikace na používání
- Správa zásad
  - Vytvoření zásad
  - Export a import zásady
  - Ukazatel úrovně zabezpečení
- Správa úloh
- Konfigurace místních nastavení aplikace
- Spuštění a zastavení aplikace Kaspersky Endpoint Security
- Pozastavení a obnovení ochrany a kontroly počítače
- Vytvoření nebo použití konfiguračního souboru
- Obnovení výchozího nastavení aplikace
- Výkon aplikace Kaspersky Endpoint Security a kompatibilita s jinými aplikacemi
  - Povolení nebo zakázání režimu úspory energie
  - Povolení nebo zakázání uvolnění prostředků pro jiné aplikace
  - Doporučené postupy pro optimalizaci výkonu aplikace Kaspersky Endpoint Security

Kontrola malwaru
- Kontrola počítače
- Kontrola vyměnitelných jednotek připojených k počítači
- Kontrola na pozadí
- Kontrola z místní nabídky
- Kontrola integrity aplikace
- Úprava rozsahu kontroly
- Spuštění naplánované kontroly
- Spuštění kontroly jako jiný uživatel
- Optimalizace kontroly

Aktualizace databází a softwarových modulů aplikace
- Scénáře aktualizace databázového a aplikačního modulu
  - Aktualizace ze serverového úložiště
  - Aktualizace ze sdílené složky
  - Aktualizace pomocí nástroje Kaspersky Update Utility
  - Aktualizace v mobilním režimu
- Spuštění a zastavení úlohy aktualizace
- Spuštění úlohy aktualizace za použití oprávnění jiného uživatelského účtu
- Volba režimu spuštění úlohy aktualizace
- Přidání zdroje aktualizací
- Aktualizace modulů aplikace
- Použití proxy serveru pro aktualizace
- Vrácení změn provedených poslední aktualizací

Technologie pokročilé dezinfekce
- Dezinfekce aktivních hrozeb na pracovních stanicích
- Dezinfekce aktivních hrozeb na serverech

Eliminace nezpracovaných hrozeb

Ochrana počítače
- Ochrana před souborovými hrozbami
  - Povolení a zakázání součásti Ochrana před souborovými hrozbami
  - Automatické pozastavení součásti Ochrana před souborovými hrozbami
  - Změna akce, kterou součást Ochrana před souborovými hrozbami provede s infikovanými soubory
  - Vytvoření rozsahu ochrany součásti Ochrana před souborovými hrozbami
  - Použití metod kontroly
  - Použití technologií kontroly při provozu součásti Ochrana před souborovými hrozbami
  - Optimalizace kontroly souborů
  - Kontrola složených souborů
  - Změna režimu kontroly
  - Kontrola kontejneru
- Prevence narušení hostitele
  - Povolení a zakázání součásti Prevence narušení hostitele
  - Správa skupin důvěryhodnosti aplikací
    - Změna skupiny důvěryhodnosti aplikace
    - Konfigurace práv skupiny důvěryhodnosti
    - Výběr skupiny důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security
    - Výběr skupiny důvěryhodnosti pro neznámé aplikace
    - Výběr skupiny důvěryhodnosti pro digitálně podepsané aplikace

- Konfigurace oprávnění aplikací
- Ochrana prostředků operačního systému a osobních údajů
- Odstraňování informací o nepoužívaných aplikacích
- Sledování součásti Prevence narušení hostitele
- Ochrana přístupu ke zvuku a videu

Ochrana před útoky BadUSB
- Povolení a zakázání součásti Ochrana před útoky BadUSB
- Zakázání používání klávesnice na obrazovce k autorizaci zařízení USB
- Autorizace čtečky čárových kódů

Ochrana AMSI
- Povolení a zakázání součásti Ochrana AMSI
- Optimalizace kontroly souborů součástí Ochrana AMSI

Ochrana před webovými hrozbami
- Povolení a zakázání součásti Ochrana před webovými hrozbami
- Konfigurace způsobů zjišťování škodlivých webových adres
- Anti-Phishing
- Vytvoření seznamu důvěryhodných webových adres
- Export a import seznamu důvěryhodných webových adres

Ochrana před hrozbami v poště
- Povolení a zakázání součásti Ochrana před hrozbami v poště
- Změna akce, která bude provedena s infikovanými e-mailovými zprávami
- Vytvoření rozsahu ochrany součásti Ochrana před hrozbami v poště
- Kontrola složených souborů přiložených k e-mailovým zprávám
- Filtrování příloh e-mailových zpráv
- Export a import rozšíření pro filtrování příloh
- Kontrola e-mailů v aplikaci Microsoft Office Outlook
- Kontrola e-mailů v aplikacích Thunderbird, MyOffice a R7-Office

Ochrana před síťovými hrozbami
- Povolení a zakázání součásti Ochrana před síťovými hrozbami
- Blokování útočícího počítače
- Konfigurace adres výjimek z blokování
- Export a import seznamu výjimek z blokování
- Konfigurace součásti Ochrana před síťovými hrozbami podle typu

Brána firewall
- Povolení a zakázání brány firewall
- Změna typu připojení k síti
- Správa pravidel síťových paketů
  - Vytváření pravidla síťových paketů
  - Povolení a zakázání pravidla síťových paketů
  - Změna akce brány firewall pro pravidlo síťových paketů
  - Změna priority pravidla síťových paketů
  - Export a import pravidel síťových paketů
  - Definování pravidel síťových paketů v jazyce XML
- Správa pravidel sítě aplikací
  - Vytváření pravidla sítě aplikací
  - Povolení a zakázání pravidla sítě aplikace
  - Změna akce brány firewall pro pravidlo sítě aplikace
  - Změna priority pravidla sítě aplikace
- Sledování sítě

Prevence zneužití
- Povolení a zakázání součásti Prevence zneužití
- Ochrana paměti systémových procesů

Detekce chování

Anti-Cryptor
- Povolení a zakázání ochrany sdílených složek proti externímu šifrování
- Konfigurace doby blokování nedůvěryhodného počítače
- Úprava rozsahu ochrany
- Přidávání důvěryhodných počítačů pro externí šifrování dat
- Export a import seznamu výjimek z ochrany sdílených složek před externím šifrováním

Modul pro nápravu

Kaspersky Security Network
- Povolení a zakázání používání služby Kaspersky Security Network

- Omezení služby Kaspersky Private Security Network
- Povolení a zakázání režimu cloudu pro součásti ochrany
- Nastavení proxy serveru KSN
- Kontrola důvěryhodnosti souboru ve službě Kaspersky Security Network
- Kontrola šifrovaných připojení
  - Povolení kontroly šifrovaného připojení
  - Instalace důvěryhodných kořenových certifikátů
  - Kontrola šifrovaných připojení s nedůvěryhodným certifikátem
  - Přidání certifikátu Kaspersky do vlastního úložiště certifikátů
  - Vyloučení šifrovaných připojení z kontroly
- Výmaz dat

Kontrola počítače

- Kontrola webu
  - Přidání pravidla přístupu k webovým prostředkům
  - Filtrování podle adres webových prostředků
  - Filtrování podle obsahu webových prostředků
  - Testování pravidel přístupu k webovým prostředkům
  - Export a import pravidel součásti Kontrola webu
  - Export a import adres webových prostředků pravidla Kontrola webu
  - Sledování aktivity uživatelů na internetu
  - Úprava šablon zpráv součásti Kontrola webu
  - Úprava masek pro adresy webových prostředků
  - Kontrola webu pro virtuální počítače
  - Proměnné v šablonách zpráv součásti Kontrola webu
- Kontrola zařízení
  - O pravidlech přístupu
  - Správa přístupu k zařízením podle typu
  - Správa přístupu k zařízením pomocí připojovací sběrnice
  - Rozlišení přístupových práv uživatelů k zařízením
  - Správa přístupu k mobilním zařízením
  - Správa přístupu k zařízením Bluetooth
  - Ovládání tisku
  - Ovládání připojení k Wi-Fi
  - Monitorování využití vyměnitelných jednotek
  - Změna doby ukládání do mezipamětintrol
  - Akce využívající důvěryhodná zařízení
    - Přidání zařízení na seznam důvěryhodných z rozhraní aplikace
    - Přidání zařízení na seznam důvěryhodných z rozhraní aplikace Kaspersky Security Center
    - Export a import seznamu důvěryhodných zařízení
  - Získání přístupu k blokovanému zařízení
    - Online režim pro udělení přístupu
    - Offline režim pro udělení přístupu
  - Úprava šablon zpráv součásti Kontrola zařízení
  - Anti-Bridging
    - Povolení součásti Anti-Bridging
    - Změna stavu pravidla připojení
    - Změna priority pravidla připojení
- Adaptivní kontrola anomálií
  - Zkušební režim součásti Adaptivní kontrola anomálií
  - Povolení a zakázání pravidla součásti Adaptivní kontrola anomálií
  - Úprava akce provedené při spuštění pravidla součásti Adaptivní kontrola anomálií
  - Vytvoření výjimky pro pravidlo součásti Adaptivní kontrola anomálií
  - Export a import výjimek pro pravidla součásti Adaptivní kontrola anomálií
  - Použití aktualizací pravidel součásti Adaptivní kontrola anomálií
  - Úprava šablon zpráv součásti Adaptivní kontrola anomálií
  - Sledování operací součásti Adaptivní kontrola anomálií
- Kontrola aplikací
  - Omezení funkcí součásti Kontrola aplikací
  - Získávání informací o aplikacích nainstalovaných v počítačích uživatelů
  - Jak povolit režim Blokované aplikace
  - Kontrola aplikací založená na počítači se základním stavem
  - Správa pravidel součásti Kontrola aplikací

Přidání podmínky aktivace pro pravidlo součásti Kontrola aplikací
Přidání spustitelných souborů ze složky Executable files do kategorie aplikací
Přidání spustitelných souborů souvisejících s událostmi do kategorie aplikací
Přidání pravidla součásti Kontrola aplikací
Změna stavu pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center
Export a import pravidel součásti Kontrola aplikací
Zobrazení událostí vyplývajících z provozu součásti Kontrola aplikací
Zobrazení zprávy o blokovaných aplikacích
Testování pravidel součásti Kontrola aplikací
Povolení a zakázání testování pravidel součásti Kontrola aplikací
Zobrazení zprávy o blokovaných aplikacích v testovacím režimu
Zobrazení událostí vyplývajících z testovacího provozu součásti Kontrola aplikací
Monitor aktivity aplikací
Pravidla pro vytváření masek názvů pro soubory nebo složky
Úprava šablon zpráv součásti Kontrola aplikací
Proměnné v šablonách zpráv součásti Kontrola aplikací
Osvědčené postupy pro implementaci seznamu povolených aplikací
Konfigurace režimu seznamu povolených položek pro aplikace
Testování režimu seznamu povolených položek
Podpora režimu seznamu povolených položek
Monitorování síťových portů
Povolení monitorování všech síťových portů
Vytvoření seznamu sledovaných síťových portů
Vytvoření seznamu aplikací, pro které jsou sledovány všechny síťové porty
Export a import seznamů sledovaných portů
Kontrola protokolu
Konfigurace předdefinovaných pravidel
Přidávání vlastních pravidel
Monitorování integrity systému
O pravidlech součásti Monitorování integrity systému
Monitorování integrity systému v reálném čase
Kontrola integrity systému na vyžádání
Export a import pravidel součásti Monitorování integrity systému
Zobrazení zpráv součásti Monitorování integrity systému
Obnovení stavu integrity systému
Cloud Discovery
Důvěryhodná zóna
Vytvoření výjimky z kontroly
Vytvoření výjimky podle typu zjištěných objektů
Úprava seznamu důvěryhodných aplikací
Vytvoření místní důvěryhodné zóny
Export a import důvěryhodné zóny
Zpracování aplikací s důvěryhodným digitálním podpisem
Příloha Předdefinované výjimky z kontroly a důvěryhodné aplikace
Server SQL
Server Microsoft Exchange
System Center Configuration Manager
Citrix
VMware
Správa zálohy
Konfigurace maximální doby uložení souborů v záloze
Konfigurace maximální velikosti zálohy
Obnovení souborů ze zálohy
Odstranění záložních kopií souborů ze zálohy
Oznamovací služba
Konfigurace nastavení protokolů událostí
Konfigurace zobrazení a doručování upozornění
Konfigurace zobrazení varování v oznamovací oblasti, která se týkají stavu aplikace
Zasílání zpráv mezi uživateli a správcem
Správa zpráv
Zobrazení sestav
Konfigurace maximální doby uchovávání zpráv

- Konfigurace maximální velikosti souboru zprávy
- Uložení zprávy do souboru
- Mazání zpráv

Sebeobrana aplikace Kaspersky Endpoint Security
- Povolení a zakázání sebeobrany
- Povolení a zakázání podpory technologie AM-PPL
- Ochrana služeb aplikace před externí správou
- Podpora aplikací vzdálené správy
- Ochrana heslem
  - Povolit ochranu heslem
  - Udělení oprávnění jednotlivým uživatelům nebo skupinám
  - Použití dočasného hesla k udělení oprávnění
  - Rušení dočasného hesla
  - Zvláštní aspekty oprávnění týkajících se ochrany heslem
  - Resetování hesla KLAdmin
- Ochrana připojení k serveru pro správu

Šifrování dat
- Omezení funkce šifrování
- Změna délky šifrovacího klíče (AES56/AES256)
- Kaspersky Disk Encryption
  - Zvláštní funkce šifrování jednotky SSD
  - Spuštění nástroje Kaspersky Disk Encryption
  - Vytvoření seznamu pevných disků vyloučených ze šifrování
  - Export a import seznamu pevných disků vyloučených ze šifrování
  - Povolení technologie SSO (Single Sign-On)
  - Správa účtů ověřovacího agenta
  - Použití tokenu a čipové karty v kombinaci s ověřovacím agentem
  - Dešifrování pevných disků
  - Obnovení přístupu k jednotce chráněné technologií Kaspersky Disk Encryption
  - Přihlášení pomocí účtu služby ověřovacího agenta
  - Aktualizace operačního systému
  - Odstranění chyb aktualizace funkce šifrování
  - Trasování ověřovacího agenta
  - Úprava textů nápovědy pro ověřovacího agenta
  - Odstranění zbylých objektů a dat po testování činnosti ověřovacího agenta
- Správa nástroje BitLocker
  - Spuštění nástroje BitLocker Drive Encryption
  - Dešifrování pevného disku chráněného nástrojem BitLocker
  - Obnovení přístupu k pevnému disku chráněnému nástrojem BitLocker
  - Pozastavení ochrany BitLocker kvůli aktualizaci softwaru
- Šifrování na úrovni souborů na místních discích počítače
  - Šifrování souborů na místních počítačových discích
  - Vytvoření pravidel přístupu k šifrovaným souborům pro aplikace
  - Šifrování souborů vytvořených nebo upravených konkrétními aplikacemi
  - Generování pravidla dešifrování
  - Dešifrování souborů na místních počítačových discích
  - Vytvoření šifrovaných balíčků
  - Blokování přístupu k šifrovaným souborům
  - Obnovení přístupu k šifrovaným datům po selhání operačního systému
  - Úprava šablon zpráv pro přístup k šifrovaným souborům
- Šifrování vyměnitelných jednotek
  - Spuštění šifrování vyměnitelných jednotek
  - Přidání pravidla šifrování pro vyměnitelné jednotky
  - Export a import seznamu pravidel šifrování pro vyměnitelné jednotky
  - Přenosný režim pro přístup k šifrovaným souborům na vyměnitelných jednotkách
  - Dešifrování vyměnitelných jednotek
- Zobrazení podrobností o šifrování dat
  - Zobrazení stavu šifrování
  - Zobrazení statistik šifrování na řídicích panelech aplikace Kaspersky Security Center
  - Zobrazení chyb šifrování souborů na místních discích počítače
  - Zobrazení zprávy šifrování dat
- Práce s šifrovanými zařízeními v případě, že není k dispozici žádný přístup k nim

- Obnova dat pomocí nástroje pro obnovení FDERT
- Vytvoření záchranného disku operačního systému

Řešení Detection and Response

- Licence k MDR a EDR Optimum
- Kompatibilita s řešeními EDR třetích stran
- Kaspersky Endpoint Agent
  - Migrace konfigurace [KES+KEA] na konfiguraci [KES+integrovaný agent]
  - Migrace zásad a úloh pro Kaspersky Endpoint Agent
- Endpoint Detection and Response Agent (EDR Agent)
  - Instalace aplikace EDR Agent
  - Integrace aplikace EDR Agent s MDR
  - Integrace aplikace EDR Agent s EDR (KATA)
  - Integrace aplikace EDR Agent s NDR (KATA)
  - Integrace aplikace EDR Agent s EDR Expert (on-premise)
  - Kompatibilita s aplikacemi EPP třetích stran
- Managed Detection and Response
  - Integrace integrovaného agenta s MDR
  - Průvodce migrací KEA na KES pro MDR
- Endpoint Detection and Response
  - Integrace integrovaného agenta s EDR Optimum / EDR Expert
  - Vyhledávání indikátorů narušení (standardní úloha)
  - Rozšířená telemetrie pro Kontrolu IOC
  - Přesunout soubor do karantény
  - Načíst soubor
  - Odstranit soubor
  - Zahájení procesu
  - Ukončit proces
  - Prevence spouštění
  - Izolace počítače od sítě
  - Cloud Sandbox
  - Průvodce migrací KEA na KES pro EDR Optimum
- Kaspersky Sandbox
  - Integrace integrovaného agenta s řešením Kaspersky Sandbox
  - Vyhledávání indikátorů narušení (samostatná úloha)
  - Průvodce migrací KEA na KES pro Kaspersky Sandbox
- Kaspersky Anti Targeted Attack Platform
  - Integrace integrovaného agenta s EDR/NDR (KATA)
  - Konfigurace telemetrie EDR (KATA)
  - Výjimky z telemetrie EDR (KATA)
    - Příklad 1. Vyloučené procesy
    - Příklad 2. Vyloučená síťová komunikace
    - Příklad 3. Vyloučené operace se souborem
    - Příklad 4. Vyloučené změny registru
  - KATA Sandbox
    - Integrace integrovaného agenta s řešením KATA Sandbox
    - Konfigurace akcí součásti Reakce na hrozbu
  - Průvodce migrací KEA na KES pro EDR (KATA)
- Endpoint Detection and Response Expert (on-premise)
  - Integrace integrovaného agenta s řešením EDR Expert (on-premise)
  - Konfigurace nastavení telemetrie EDR Expert (on-premise)
  - Výjimky z telemetrie EDR Expert (on-premise)
  - Export a import filtrů událostí EDR Expert (on-premise)
- Správa karantény
  - Konfigurace maximální velikosti karantény
  - Odesílání dat o souborech v karanténě do aplikace Kaspersky Security Center
  - Obnovení souborů z karantény
- Monitorování akcí EDR

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

- Integrace aplikace Kaspersky Endpoint Security s KUMA
- Filtrování událostí, které mají být odeslány do sítě KUMA
- Export a import filtrů událostí KUMA

Průvodce migrací z KSWS na KES

- Shoda součástí KSWS a KES
- Shoda nastavení KSWS a KES
- Migrace součástí KSWS
- Migrace úloh a zásad KSWS
- Migrace důvěryhodné zóny KSWS
- Migrace pravidel součásti KSWS Kontrola spouštění aplikací
- Instalace KES místo KSWS
- Migrace konfigurace [KSWS+KEA] na konfiguraci [KES+integrovaný agent]
- Ověření, že aplikace Kaspersky Security for Windows Server byla úspěšně odebrána
- Aktivace KES pomocí klíče KSWS
- Zvláštní aspekty migrace serverů s vysokou zátěží
- Správa aplikace na serveru v režimu Server Core
- Migrace z [KSWS+KEA] na [KES+integrovaný agent]

Režim Light Agent pro ochranu virtuálních počítačů

- Zvláštní opatření pro režim Light Agent
- Předběžná konfigurace virtuálního počítače
  - Kompatibilita s technologií Citrix App Layering
  - Kompatibilita s technologií Citrix Provisioning (Citrix Provisioning Services)
  - Kompatibilita s technologií Omnissa App Volumes
- Instalace součásti Light Agent
- Připojování součásti Light Agent k SVM
  - Zjištění SVM
  - Konfigurace algoritmu výběru SVM pro součást Light Agent
  - Distribuce připojení součástí Light Agent k součástem SVM (značky)
  - Ochrana připojení mezi součástí Light Agent a SVM
- Aktivace součásti Light Agent
- Příručka migrace součásti KSVLA Light Agent na KES Light Agent
  - Instalace součásti KES Light Agent namísto součásti KSVLA Light Agent
  - Shoda součástí KSVLA Light Agent a KES Light Agent
  - Migrace úloh a zásad součásti KSVLA Light Agent
  - Migrace konfigurace [KSVLA Light Agent+KEA] na konfiguraci [KES Light Agent+integrovaný agent]

Správa aplikace z příkazového řádku

- Setup. Instalace aplikace
- Setup /x. Odebrání aplikace
- msiexec /i. Obnovení aplikace
- Příkazy AVP
  - SCAN. Kontrola malwaru
  - UPDATE. Aktualizace databází a softwarových modulů aplikace
  - ROLLBACK. Vrácení změn provedených poslední aktualizací
  - TRACES. Trasování
  - START. Spuštění profilu
  - STOP. Zastavení profilu
  - STATUS. Stav profilu
  - STATISTICS. Statistiky provozu profilu
  - RESTORE. Obnovení souborů ze zálohy
  - EXPORT. Export nastavení aplikace
  - IMPORT. Import nastavení aplikace
  - ADDKEY. Použití souboru klíče
  - LICENSE. Správa licence
  - RENEW. Zakoupení licence
  - PBATESTRESET. Resetování výsledků kontroly disku před šifrováním disku
  - EXIT. Ukončení aplikace
  - EXITPOLICY. Zakázání zásad
  - STARTPOLICY. Povolení zásad
  - DISABLE. Zakázání ochrany
  - SPYWARE. Detekce spywaru
  - KSN. Přepínání mezi KSN/KPSN
  - SERVERBINDINGDISABLE. Zákaz ochrany připojení k serveru
- Příkazy KESCLI
  - Scan. Kontrola malwaru
  - GetScanState. Stav provádění kontroly
  - GetLastScanTime. Stanovení času dokončení kontroly

GetThreats. Získání údajů o zjištěných hrozbách
UpdateDefinitions. Aktualizace databází a softwarových modulů aplikace
GetDefinitionState. Určení data a času poslední aktualizace databází
EnableRTP. Povolování ochrany
GetRealTimeProtectionState. Stav součásti Ochrana před souborovými hrozbami
GetEncryptionState. Stav šifrování disku
Version. Určení verze aplikace
Příkazy pro součást Detection and Response
SANDBOX. Správa součásti Sandbox
PREVENTION. Správa Prevence spouštění
ISOLATION. Správa izolace sítě
RESTORE. Obnovení souborů z karantény
IOCSCAN. Vyhledávání indikátorů narušení (IOC)
MDRLICENSE. Aktivace MDR
EDRKATA. Integrace s EDR (KATA)
KUMA. Integrace s KUMA
YARA. Spuštění kontroly YARA
TELEMETRYFILTERS. Filtrování událostí, které mají být odeslány do sítě KUMA
Příkazy pro správu součásti Light Agent
KSVLAINFO. Určení režimu součásti Light Agent
VIISINFO. Stav připojení součásti Light Agent k integračnímu serveru
SVMINFO. Stav připojení součásti Light Agent k serveru pro ochranu
Chybové kódy
Příloha Profily aplikací
Správa aplikace prostřednictvím rozhraní REST API
Instalace aplikace pomocí rozhraní REST API
Práce s API
Zdroje informací o aplikaci
Kontaktování technické podpory
Obsah a uložení souborů trasování
Trasování provozu aplikace
Trasování výkonu aplikace
Zápis souborů výpisu
Ochrana souborů výpisu a trasovacích souborů
Načítání dat operačního systému (Kaspersky Get System Info)
Omezení a varování
Slovníček pojmů
Aktivní klíč
Antivirové databáze
Archiv
Cloud Discovery
Databáze phishingových webů
Databáze škodlivých webových adres
Dezinfekce
Falešný alarm
Infikovaný soubor
Infikovatelný soubor
Integrační server
IOC
Licenční certifikát
Light Agent
Maska
Mobilní správce souborů
Network Agent
Normalizovaná forma adresy webového prostředku
Objekt OLE
OpenIOC
Ověřovací agent
Ověřování protokolem Kerberos
Rozsah kontroly
Rozsah ochrany
Skupina správy

- Soubor IOC
- SVM
- Trusted Platform Module
- Úloha
- Vystavitel certifikátu

Přílohy

- Příloha 1. Nastavení aplikace
  - Ochrana před souborovými hrozbami
  - Ochrana před webovými hrozbami
  - Ochrana před hrozbami v poště
  - Ochrana před síťovými hrozbami
  - Brána firewall
  - Ochrana před útoky BadUSB
  - Ochrana AMSI
  - Prevence zneužití
  - Detekce chování
  - Prevence narušení hostitele
  - Modul pro nápravu
  - Kaspersky Security Network
  - Kontrola protokolu
  - Anti-Cryptor
  - Kontrola webu
  - Kontrola zařízení
  - Kontrola aplikací
  - Adaptivní kontrola anomálií
  - Monitorování integrity systému
  - Endpoint Sensor
  - Sandbox
  - Managed Detection and Response
  - Endpoint Detection and Response
  - Endpoint Detection and Response Expert (on-premise)
  - Network Detection and Response (KATA)
  - Integrace s KUMA
  - Úplné šifrování disku
  - Šifrování na úrovni souborů
  - Šifrování vyměnitelných jednotek
  - Šablony (šifrování dat)
  - Výjimky
  - Nastavení aplikace
  - Zprávy a úložiště
  - Nastavení sítě
  - Rozhraní
  - Správa nastavení
  - Aktualizace databází a softwarových modulů aplikace
- Příloha 2. Skupiny důvěryhodnosti aplikací
- Příloha 3. Přípony souborů pro rychlou kontrolu vyměnitelných jednotek
- Příloha 4. Typy souborů pro filtr příloh Ochrana před hrozbami v poště
- Příloha 5. Nastavení sítě pro interakci s externími službami
- Příloha 6. Události aplikace
  - Kritické
  - Chyby funkcí
  - Varování
  - Informační zpráva
- Příloha 7. Podporované přípony souborů pro součást Prevence spouštění
- Příloha 8. Podporované překladače skriptů pro součást Prevence spouštění
- Příloha 9. Rozsah kontroly IOC v registru (RegistryItem)
- Příloha 10. Požadavky na soubor IOC
- Příloha 11. Uživatelské účty v pravidlech součástí aplikace
- Příloha 12. Rozhraní API pro reakci na hrozby EDR

Informace o kódu třetích stran

Informace o ochranných známkách

Nápověda k aplikaci Kaspersky Endpoint Security pro systém Windows

Co je nového ve verzi 14.0

- Podpora pro počítače s architekturou ARM
- Podpora pro revize zásad za účelem auditu změn parametrů zásad
- Co je nového v jednotlivých verzích Kaspersky Endpoint Security pro systém Windows

Eliminace hrozeb

- Na pracovních stanicích
- Na serverech
- Reakce na zjištění indikátoru narušení (Izolace sítě → Karanténa → Prevence spouštění)

Začínáme

- Nasazení aplikace Kaspersky Endpoint Security pro systém Windows
- Počáteční nastavení aplikace Kaspersky Endpoint Security pro systém Windows
- Licence k aplikaci Kaspersky Endpoint Security pro systém Windows

Doporučené postupy

- Optimalizace výkonu aplikací
- Implementace režimu Standardně odmítat v součásti Kontrola aplikací
- Migrace KEA na KES s integrovaným agentem

Poskytování údajů

- Na základě licenční smlouvy s koncovým uživatelem
- Při používání KSN
- GDPR

Použití KES jako součást jiných řešení

- Kaspersky EDR
- Kaspersky Sandbox
- Kaspersky MDR

Co je nového

Rozbalit vše | Sbalit vše

Aktualizace 14.0

Aplikace Kaspersky Endpoint Security 14.0 pro systém Windows zavádí následující funkce a vylepšení:

1. Nově jsou podporovány počítače s architekturou ARM. Aplikaci můžete nainstalovat buď ve standardním režimu, nebo v režimu EDR Agent. Aplikace má však několik omezení (například z technologií šifrování dat je podporován pouze BitLocker).
2. Ve webové konzole aplikace Kaspersky Security Center verze 15.0 nebo novější je podporován rozšířený audit zásad. Nově si můžete prohlédnout revize zásad a uložit je do souboru. *Revize* je soubor změněných parametrů uložených uživatelem. Revize umožňují porovnat a vrátit změny parametrů zásad.
3. Pro uživatele aplikace Kaspersky Endpoint Detection and Response jsou nově k dispozici nové události telemetrie. Tyto nové události vylepšují možnosti zjišťování hrozeb řešením Kaspersky EDR.
4. Při vývoji této verze aplikace Kaspersky Endpoint Security pro systém Windows jsme zapracovali změny zahrnuté v následujících soukromých opravách: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Aktualizace 12.12

Aplikace Kaspersky Endpoint Security 12.12 pro systém Windows zavádí následující funkce a vylepšení:

1. Ochrana sdílených složek před externím šifrováním, která bývala součástí součásti Detekce chování, je nyní samostatnou součástí, Anti-Cryptor.

2. Byla přidána podpora pro protokol Kerberos za účelem ověření aplikace prostřednictvím proxy serveru pro přístup k internetu.

3. Nově můžete určit hodnotu hash souboru pro důvěryhodnou aplikaci, a nejen úplnou cestu.

4. Uživatelům řešení EDR (Endpoint Detection and Response) je k dispozici více funkcí úlohy *Kontrola IOC*. Nově je k dispozici funkce Retrospektivní kontrola IOC. *Retrospektivní kontrola IOC* je režim úlohy *Kontrola IOC*, ve kterém aplikace Kaspersky Endpoint Security kontroluje indikátory narušení pomocí dat za určité časové období. Tento režim je určen pro zjišťování indikátorů narušení v datech o síťové aktivitě počítače. Kaspersky Endpoint Security analyzuje data v protokolech operačního systému a protokolech prohlížeče v počítači.

5. Uživatelé řešení Kaspersky Endpoint Detection and Response (EDR) mohou odebrat limit velikosti karantény. To může být nutné u kontroly YARA, protože aplikace může uložit velký soubor výpisu paměti. Nově můžete použít pro karanténu všechno volné místo na disku.

6. Pro optimalizaci exportu událostí na platformu KUMA (Kaspersky Unified Monitoring and Analysis Platform) je nově podporována komprese HTTPS. To pomáhá snižovat objem odchozích přenosů.

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

Aktualizace 12.11

Aplikace Kaspersky Endpoint Security 12.11 pro systém Windows nabízí následující funkce a vylepšení:

1. Aplikace před uložením nastavení zkontroluje konfiguraci součástí kontroly. Tato kontrola byla přidána pro součásti Kontrola aplikací, Kontrola zařízení a Monitorování integrity systému. Aplikace nově zobrazí varování, pokud může aktuální nastavení součásti kontroly zvýšit zátěž počítače nebo způsobit selhání systému. Pokud jste například v případě součásti Kontrola aplikací vybrali režim, který blokuje všechny aplikace kromě povolených, a nepřidali jste žádné povolovací pravidlo, aplikace zobrazí varování, protože takováto konfigurace může způsobit selhání systému.

2. Byla přidána podpora pro automatické odesílání souborů do součásti KATA Sandbox ke kontrole. *KATA Sandbox* je součást řešení Kaspersky Anti Targeted Attack Platform, která spouští soubory na virtuálních bitových kopií systémů. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Aby součást KATA Sandbox fungovala v automatickém režimu, musí být nasazena platforma Kaspersky Anti Targeted Attack Platform 8.0 nebo novější.

3. Optimalizované odesílání EDR telemetrie. Nově můžete určit maximální délku paketu.

4. Byla vylepšena diagnostika připojení ke službě Kaspersky Security Network. Za účelem řešení potenciálních problémů byly rozšířeny podrobnosti o chybách připojení pro Kaspersky Security Network.

5. Byla přidána podpora pro konfiguraci seznamů událostí, které mají být odesílány na platformu Kaspersky Unified Monitoring and Analysis Platform (KUMA). Nově můžete kromě předdefinovaných seznamů událostí na platformě KUMA ručně přidávat události do telemetrie nebo vyloučit události podle jejich ID v protokolu událostí systému Windows.

6. Bylo aktualizováno rozhraní zásad ve webové konzole. Změnilo se rozložení částí zásad pro rychlejší přístup k základním funkcím.

7. Podpora pro Windows 11 25H2.

8. Při vývoji této verze aplikace Kaspersky Endpoint Security pro systém Windows jsme zapracovali změny zahrnuté v následujících soukromých opravách: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Aktualizace 12.10

Aplikace Kaspersky Endpoint Security 12.10 pro systém Windows nabízí následující funkce a vylepšení:

1. U součásti Ochrana před útoky BadUSB byla přidána možnost autorizovat čtečky čárových kódů načtením čárového kódu z obrazovky. K autorizaci čteček čárových kódů nově není nutné zadávat kód pomocí klávesnice na obrazovce.

2. Uživatelům řešení Endpoint Detection and Response (EDR) od společnosti Kaspersky jsou k dispozici následující funkce a vylepšení:

   - Nově můžete v podrobnostech výstrahy spravovat izolaci počítače od sítě. V podrobnostech výstrahy můžete navíc určit časové období izolace počítače od sítě a přidávat výjimky.

- Vyplnění nových údajů do podrobností výstrahy. Podrobnosti výstrahy nově obsahují více informací o hrozbě, včetně toho, jak se aplikace chová při reakci na hrozby EDR.
- Bylo vylepšeno zpracování souborů IOC. Nově můžete zobrazovat a upravovat obsah souborů IOC v rozhraní webové konzoly aplikace Kaspersky Security Center. Po načtení souboru IOC aplikace zobrazí zprávu o aplikaci podmínky IOC.
- Byla vylepšena reakce na zjištěné IOC. Nově můžete do karantény umístit soubory zjištěné úlohou *Kontrola IOC* přímo ve výsledcích detekce IOC ve vlastnostech úlohy. V nastavení úlohy můžete také izolovat počítače od sítě.
- Nově můžete soubory IOC vytvářet přímo ve vlastnostech úlohy *Kontrola IOC* na základě seznamů hodnot hash souborů, IP adres nebo názvů DNS vygenerovaných v souboru TXT.
- Byl rozšířen rozsah kontroly u úlohy *Kontrola IOC*. Nově můžete definovat rozsah kontroly IOC registru (**registr systému Windows – Registryltem**). V dřívějších verzích aplikace bylo možné použít pouze rozsah kontroly IOC v registru.

3. Bylo přidáno nové oprávnění funkce Ochrana heslem, *Nastavení exportu*. Ve výchozím nastavení může pouze uživatel KLAdmin vytvořit konfigurační soubor s nastavením aplikace Kaspersky Endpoint Security v rozhraní aplikace. Chcete-li udělit přístup jiným uživatelům, musíte jim udělit příslušná oprávnění.
4. Při vývoji této verze aplikace Kaspersky Endpoint Security pro systém Windows jsme zapracovali změny zahrnuté v následujících soukromých opravách: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Aktualizace 12.9

Aplikace Kaspersky Endpoint Security 12.9 pro systém Windows nabízí následující funkce a vylepšení:

1. Byla přidána nová funkce pro *správu dočasných hesel*. Dočasné heslo vám umožňuje poskytnout přístup k aplikaci Kaspersky Endpoint Security s povolenou funkcí Ochrana heslem pro samostatný počítač. Správa dočasných hesel umožňuje ukládat historii hesel (až 30 dnů), sledovat stav dočasných hesel (*Aktivní*, *Vypršela platnost*, *Odvolané*) a odvolávat dočasná hesla.
2. Byla přidána možnost ukončit připojení k webovým prostředkům zakázaným pravidly součásti Kontrola webu ihned po použití zásad. V předchozích verzích aplikace součást Kontrola webu omezovala pouze nová připojení k zakázaným webovým zdrojům.
3. Pro uživatele platformy Kaspersky Anti Targeted Attack Platform byla přidána možnost spustit kontrolu YARA místně v počítači. K tomu si musíte stáhnout soubor s pravidly YARA a spustit příkaz v CMD.
4. Bylo opraveno chování aplikace při povolení nástroje BitLocker v počítačích, na nichž jsou již jednotky chráněny nástrojem BitLocker pomocí nástrojů třetích stran. Aplikace Kaspersky Endpoint Security zahájí proces obnovení a odešle obnovovací klíč do aplikace Kaspersky Security Center. Správa nástroje BitLocker je tedy přenesena do konzoly aplikace Kaspersky Security Center.
5. Uživatelům řešení Detection and Response je k dispozici nová část, **Response history**. Tato část obsahuje informace o akcích reakce na hrozby provedených v počítači. Mezi tyto akce patří například spuštění úlohy *Ukončit proces* nebo izolace počítače od sítě. Response history je k dispozici pouze uživatelům následujících řešení Kaspersky: MDR, EDR, KATA.
6. Pro uživatele platformy Kaspersky Unified Monitoring and Analysis Platform je nově k dispozici podpora akcí reakce na hrozby EDR. Při reakci na hrozby spouští KUMA skripty, které vytvářejí odpovídající úlohy EDR. Pokud chcete provádět úlohy EDR, musíte v konzole KUMA vytvořit pravidlo reakce pro vlastní skript a vybrat události.
7. Při vývoji této verze aplikace Kaspersky Endpoint Security pro systém Windows jsme zapracovali změny zahrnuté v následujících soukromých opravách: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Aktualizace 12.8

Aplikace Kaspersky Endpoint Security 12.8 pro systém Windows nabízí následující funkce a vylepšení:

1. Aplikace nově podporuje režim Light Agent pro ochranu virtuálních prostředí. Nově můžete aplikaci nasadit jako součást Light Agent v rámci řešení Kaspersky Security for Virtualization Light Agent 6.2.
2. Nově je podporováno zachytávání operací se soubory v kontejnerech Docker na serverech. *Kontejner* je izolované prostředí, ve kterém může být aplikace spuštěna bez přímé interakce s operačním systémem. Kaspersky Endpoint Security kontroluje soubory uvnitř kontejnerů, ke kterým uživatel získá přístup. Když je zjištěna hrozba, aplikace tuto škodlivou činnost zablokuje a pokusí se dezinfikovat soubor uvnitř kontejneru. Pokud soubor nelze dezinfikovat, aplikace kontejner zastaví.

3. Nově můžete definovat rozsah ochrany pro ochranu sdílených složek před externím šifrováním (součást Detekce chování). Nově můžete určit sdílené složky, u nichž musí aplikace sledovat aktivitu souborů. Z rozsahu ochrany můžete také vyloučit soubory. V předchozích verzích aplikace součást Detekce chování monitorovala aktivitu souborů u všech sdílených složek.

4. Nově můžete v instalačním balíčku nakonfigurovat různé sady součástí pro různé typy operačních systémů. To znamená, že aplikaci můžete nasadit na pracovní stanice a servery pomocí instalačního balíčku. Součásti, které nejsou pro určitý typ operačního systému k dispozici, jsou z vlastností instalačního balíčku automaticky vyloučeny.

5. Byla přidána možnost vybrat předdefinované výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace umožňují rychlou konfiguraci důvěryhodné zóny pro aplikaci ve virtuálním prostředí (Citrix, VMware). Mezi tyto výjimky patří například soubory virtuálního počítače VHD a VHDX. Výjimky lze přidat při vytváření instalačního balíčku aplikace, vytváření zásady nebo při instalaci aplikace Kaspersky Endpoint Security.

6. Telemetrie EDR nově zahrnuje události pro operace se zařízeními připojenými přes USB. Tyto události můžete také přidat do výjimek z telemetrie EDR.

7. Byla přidána možnost blokovat síťová připojení přes zastaralý protokol TLS 1.0. TLS 1.0 má nízkou úroveň zabezpečení, proto doporučujeme tento protokol zakázat a používat novější verze TLS 1.2 nebo TLS 1.3. Ve výchozím nastavení aplikace Kaspersky Endpoint Security blokuje připojení TLS 1.0. Po aktualizaci verze aplikace může selhat provoz služeb třetích stran, které používají protokol TLS 1.0. Chcete-li se vyhnout problémům při provozu služeb třetích stran, můžete povolit použití protokolu TLS 1.0 v zásadách skupiny před aktualizací verze aplikace.

8. Při vývoji této verze aplikace Kaspersky Endpoint Security pro systém Windows jsme zapracovali změny zahrnuté v následujících soukromých opravách: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Aktualizace 12.7

Aplikace Kaspersky Endpoint Security 12.7 pro systém Windows nabízí následující funkce a vylepšení:

1. Nově můžete omezovat využití prostředků CPU u úlohy *Kontrola malwaru*. Chcete-li to provést, v nastavení aplikace zadejte maximální procento zatížení CPU pro všechna jádra, která lze využít při kontrole počítače.

2. Nově můžete ručně odesílat soubory ke kontrole v součásti KATA Sandbox. *KATA Sandbox* je součást řešení Kaspersky Anti Targeted Attack Platform, která spouští soubory na virtuálních bitových kopií systémů. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Chcete-li odeslat soubor ke kontrole do součásti KATA Sandbox, vyberte příslušný příkaz v místní nabídce souboru.

3. Nově můžete nastavit integraci s řešením, které chrání firemní síť LAN, *Kaspersky Network Detection and Response*. Kaspersky Network Detection and Response (NDR) je součástí řešení Kaspersky Anti Targeted Attack Platform. Interakci s NDR můžete nakonfigurovat ve standardním režimu i v režimu EDR Agent.

4. Do rozšíření Ochrana před hrozbami v poště byla přidána podpora pro e-mailového klienta Microsoft Office Outlook verze 2021. Rozšíření umožňuje kontrolu zpráv na úrovni poštovního klienta namísto na úrovni protokolu. Kromě zpráv vám rozšíření umožňuje kontrolovat objekty přijaté prostřednictvím rozhraní MAPI z úložišť Microsoft Exchange (například objekty v Kalendáři). Tato kontrola probíhá v poštovním klientovi.

5. Při vývoji této verze Kaspersky Endpoint Security pro Windows jsme začlenili změny zahrnuté do následujících soukromých oprav: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Aktualizace 12.6

Aplikace Kaspersky Endpoint Security 12.6 pro systém Windows nabízí následující funkce a vylepšení:

1. Byla přidána funkce pro integraci s řešením Kaspersky SIEM – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)*. Nově je možné odesílat události z protokolů událostí systému Windows do kolektoru KUMA. To umožňuje KUMA přijímat události systému Windows (je podporována omezená sada EventID) ze všech počítačů, na kterých je nainstalována aplikace Kaspersky Endpoint Security, bez instalace agentů KUMA na tyto počítače.

2. Byla přidána nová součást *Monitorování integrity systému*, která nahrazuje součást Monitor integrity souborů. Součást Monitorování integrity systému zahrnuje veškeré funkce součásti Monitor integrity souborů a navíc umožňuje sledovat změny registru a připojení externích zařízení. Součást Monitorování integrity systému monitoruje změny v operačním systému, které mohou naznačovat narušení zabezpečení počítače. V případě zjištění takovýchto změn Kaspersky Endpoint Security vygeneruje odpovídající události a upozorní správce. Monitor integrity souborů již není součástí aplikace. Při aktualizaci aplikace se nastavení součásti Monitor integrity souborů automaticky migruje do součásti Monitorování integrity systému. Pro zajištění správného fungování součásti Monitorování integrity systému je třeba aktualizovat aplikaci Kaspersky Endpoint Security i modul plug-in administrace na verzi 12.6.

3. Do vlastností počítače v konzole aplikace Kaspersky Security Center byl přidán stav nainstalovaného integrované součásti EDR Agent (KATA). Pokud máte nainstalovanou integrovanou součást EDR Agent (KATA), ve sloupci **Stav Endpoint Sensor** se nově zobrazuje aktuální stav součásti (např. *Spuštěno*, *Zastaveno*, *Není podporováno licencí* atd.).

4. Byla přidána možnost vybrat předdefinované výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat důvěryhodnou zónu při používání aplikace na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager. Mezi tyto výjimky patří například databázové soubory MDF a LDF. Výjimky lze přidat při vytváření nové zásady, úpravě stávající zásady nebo při instalaci aplikace Kaspersky Endpoint Security.

5. Zobrazení podrobností výstrah pro řešení Kaspersky Endpoint Detection and Response Optimum bylo přesunuto z modulu plug-in pro správu aplikace Kaspersky Endpoint Security do samostatného modulu plug-in pro správu řešení Kaspersky Endpoint Detection and Response. Modul plug-in pro správu EDR je jediný modul plug-in pro práci s agenty v operačních systémech Windows, Mac a Linux. Nově budete při práci s řešením EDR Optimum pro vytváření úloh reakce na hrozby a modul pro správu EDR pro zobrazení podrobností o výstrahách potřebovat modul plug-in administrace Kaspersky Endpoint Security.

6. Podpora pro Windows 11 24H2.

7. Při vývoji této verze Kaspersky Endpoint Security pro Windows jsme začlenili změny zahrnuté do následujících soukromých oprav: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Aktualizace 12.5

Aplikace Kaspersky Endpoint Security 12.5 pro systém Windows nabízí následující funkce a vylepšení:

1. Byla přidána možnost konfigurovat výjimky telemetrie. *Telemetrie* je seznam událostí, ke kterým došlo na chráněném počítači. Telemetrická data používá Kaspersky Anti Targeted Attack Platform (EDR) k monitorování a ochraně IT infrastruktury organizace. Konfigurace výjimek telemetrie pomáhá zlepšit výkon počítače a optimalizovat přenos dat na server pro shromažďování telemetrie.

2. Bylo vylepšeno rozhraní důvěryhodné zóny aplikace. Kaspersky Endpoint Security nově před uživatelem skrývá objekty důvěryhodné zóny, pokud správce zakázal uživateli přidávat vlastní (místní) výjimky z kontroly a důvěryhodné aplikace. Tím se zabrání neoprávněnému přístupu narušitele do důvěryhodné zóny, čímž se zvýší úroveň zabezpečení počítače.

3. Byla přidána možnost kontroly provozu pro poštovní klienty MyOffice Mail a R7-Office Organizer. Součást Ochrana před hrozbami v poště nově kontroluje nejen přílohy zpráv při stahování, ale také odesílané a přijímané zprávy.

4. Byla přidána nová kategorie webových prostředků *Generativní nástroje AI*. Přístup k webům z této nové kategorie můžete nakonfigurovat pomocí součásti Kontrola webu.

5. Nově můžete vybrat umístění pravidla síťových paketů v seznamu brány firewall. Umístění pravidla síťových paketů v seznamu určuje jeho prioritu. V předchozích verzích aplikace bylo možné prioritu pravidla nastavit pouze tak, že pravidlo přidáte na konec seznamu a ručně ho v seznamu posunete. Nyní si při přidávání pravidla můžete vybrat, zda má být pravidlo umístěno na začátek, na konec seznamu nebo vedle vybraného pravidla.

6. V pravidlech součástí aplikace Kaspersky Endpoint Security nově můžete vybírat uživatele nejen z Active Directory, ale také ze seznamu uživatelů v aplikaci Kaspersky Security Center. Údaje o místním uživatelském účtu můžete zadat také ručně. Tato možnost byla přidána pro pravidla následujících součástí: Kontrola aplikací, Kontrola zařízení, Kontrola webu, Adaptivní kontrola anomálií a Kontrola protokolu.

7. Zpráva o detekci síťového útoku nyní obsahuje sloupec s MAC adresou útočícího počítače (součást Ochrana před síťovými hrozbami). Nově vidíte ve zprávě kromě IP adresy i MAC adresu útočícího počítače. To je užitečné pro vyšetřování incidentů. Zprávy obsahující adresu MAC útočícího počítače budou k dispozici také v konzole aplikace Kaspersky Security Center Linux verze 15.1 a novější.

8. Byla zvýšena úroveň požadavků na ochranu počítače. Vysoká úroveň ochrany nyní vyžaduje povolení funkce Ochrana služeb aplikace před externí správou. Indikátor úrovně zabezpečení si můžete zobrazit v horní části okna zásad. Pokud máte střední nebo nízkou úroveň zabezpečení, můžete povolit funkci Ochrana služeb aplikace před externí správou v okně doporučení indikátoru úrovně zabezpečení.

9. Byla přidána podpora pro nové události detekce objektů, když je aplikace spuštěna v konfiguraci Endpoint Detection and Response Agent (EDR Agent). Tyto události už byly podporovány v konfiguraci [KES+integrovaný agent].

10. Při vývoji této verze Kaspersky Endpoint Security pro Windows jsme začlenili změny zahrnuté do následujících soukromých oprav: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Aktualizace 12.4

Aplikace Kaspersky Endpoint Security 12.4 pro systém Windows nabízí následující funkce a vylepšení:

1. Byla přidána nová funkce pro ochranu připojení počítače k aplikaci Kaspersky Security Center. Nová úloha *Ochrana připojení k serveru pro správu* umožňuje nastavení hesla pro připojení k důvěryhodnému serveru. To znamená, že bez tohoto hesla není možné počítač znovu připojit a spouštět příkazy z jiného serveru.

2. U součásti Ochrana heslem byla přidána možnost vybírat uživatele ručně, a ne pouze z Active Directory. To znamená, že můžete ručně zadat uživatelské jméno a heslo a udělit přístupová práva k aplikaci Kaspersky Endpoint Security pro tento účet. Pro řízení přístupu k aplikaci tak nemusíte sdílet heslo KLAdmin s ostatními uživateli ani vytvářet nové účty služby Active Directory.

3. Podpora pro Windows 11 23H2.

Aktualizace 12.3

Aplikace Kaspersky Endpoint Security 12.3 pro systém Windows nabízí následující funkce a vylepšení:

1. Nově můžete aplikaci nainstalovat do konfigurace agenta Endpoint Detection and Response Agent. Tato konfigurace umožňuje instalaci aplikace se sadou součástí požadovaných řešeními Detection and Response od společnosti Kaspersky: Kaspersky Managed Detection and Response a Kaspersky Anti Targeted Attack Platform (EDR). Aplikaci v této konfiguraci můžete nainstalovat vedle řešení třetích stran (například Dr.Web, Dallas Lock, ESET). To vám umožní používat spolu s řešením Detection and Response od společnosti Kaspersky nástroje zabezpečení infrastruktury třetích stran.

2. Bylo vylepšeno fungování aplikace Kaspersky Endpoint Security se zařízeními Bluetooth. Nově můžete konfigurovat výjimky a omezit přístup ke všem zařízením Bluetooth kromě vstupních zařízení (bezdrátové klávesnice, myši atd.).

3. Byl optimalizován provoz součásti Kontrola aplikací s databázemi spustitelných souborů. Aplikace Kaspersky Endpoint Security nově automaticky odebírá informace o souboru z databáze, pokud je tato aplikace odebrána z počítače. To umožňuje udržovat databázi aktuální a šetřit prostředky aplikace Kaspersky Security Center.

4. Byla zvýšena úroveň požadavků na ochranu počítače. Vysoká úroveň ochrany nyní vyžaduje povolení ochrany heslem. Indikátor úrovně zabezpečení si můžete zobrazit v horní části okna zásad. Pokud máte střední nebo nízkou úroveň ochrany, můžete v okně doporučení indikátoru úrovně zabezpečení povolit ochranu heslem.

5. Byla přidána podpora protokolu HTTPS, aby aplikace mohla spolupracovat se službou Kaspersky Security Network. Používání HTTPS můžete povolit ve vlastnostech serveru pro správu v nastavení proxy serveru KSN.

Aktualizace 12.2

Aplikace Kaspersky Endpoint Security 12.2 pro systém Windows nabízí následující funkce a vylepšení:

1. Pro řízení připojení k Wi-Fi sítím byla přidána podpora protokolu WPA3 (Kontrola zařízení). Nově můžete v nastavení důvěryhodné Wi-Fi sítě zvolit protokol WPA3 a odmítnout připojení k síti pomocí méně zabezpečeného protokolu.

2. Nově si můžete vybrat protokol a porty pro výjimky součásti Ochrana před síťovými hrozbami. Nově můžete kromě zadání IP adres důvěryhodných zařízení také vybrat port a protokol. To vám umožní vyloučit jednotlivé datové toky a zabránit síťovým útokům z důvěryhodných IP adres.

3. *Jiné pořadí zdrojů aktualizací pro místní úlohu Aktualizace databází a modulů aplikace*, pokud je na počítač aplikována zásada. Server Kaspersky Security Center se nově ve výchozím nastavení používá jako první zdroj aktualizací namísto serverů Kaspersky. To pomáhá šetřit provoz, když uživatel spustí místní úlohu *Aktualizace databází a modulů aplikace*.

Aktualizace 12.1

Aplikace Kaspersky Endpoint Security 12.1 pro systém Windows nabízí následující funkce a vylepšení:

1. Byl přidán integrovaný agent pro řešení Kaspersky Anti Targeted Attack Platform. Pro používání řešení EDR (KATA) už nepotřebujete aplikaci Kaspersky Endpoint Agent. Všechny funkce aplikace Kaspersky Endpoint Agent bude provádět aplikace Kaspersky Endpoint Security. Pro migraci zásad aplikace Kaspersky Endpoint Agent použijte průvodce migrací. Po aktualizaci se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odebere aplikaci Kaspersky Endpoint Agent. Řešení Kaspersky Endpoint Agent bylo přidáno na seznam nekompatibilního softwaru. Kaspersky Endpoint Security má integrované agenty pro všechna řešení Detection and Response, takže instalace aplikace Kaspersky Endpoint Agent pro integraci s těmito řešeními již není nutná.

2. Nově je podporován režim kompatibility Azure WVD. Tato funkce zajišťuje správné zobrazení stavu virtuálního počítače Azure v konzole Kaspersky Anti Targeted Attack Platform. Režim kompatibility Azure WVD umožňuje těmto virtuálním počítačům přiřadit trvalé jedinečné ID senzoru.

3. Nově můžete konfigurovat uživatelský přístup k mobilním zařízením v aplikaci iTunes nebo podobných aplikacích. To znamená, že můžete například povolit použití mobilního zařízení pouze v iTunes a zablokovat používání mobilního zařízení jako vyměnitelného disku. Tato pravidla podporuje aplikace také pro aplikaci Android Debug Bridge (ADB).

4. Aplikace Kaspersky Security Center verze 11 již není podporována. Upgradujte aplikaci Kaspersky Security Center na nejnovější verzi.

Často kladené dotazy

OBECNÉ

Na jakých počítačích může aplikace Kaspersky Endpoint Security fungovat?

INTERNET

Prohledává aplikace Kaspersky Endpoint Security šifrovaná připojení (HTTPS)?

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 kontrolu malwaru, 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?

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?

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.

Aplikace není určena pro použití v technologických procesech, které zahrnují automatizované řídicí systémy. K ochraně zařízení v takových systémech doporučujeme používat aplikaci Kaspersky Industrial CyberSecurity for Nodes.

Technologie detekce hrozeb

Strojové učení

Kaspersky Endpoint Security používá model založený na strojovém učení. Tento model je vyvíjen odborníky společnosti Kaspersky. Následně jsou do modelu průběžně přidávány údaje o hrozbách ze služby KSN (trénování modelu).

Cloudová analýza

Kaspersky Endpoint Security přijímá 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.

Analýza chování

Kaspersky Endpoint Security analyzuje aktivitu objektu v reálném čase.

Automatická analýza

Kaspersky Endpoint Security přijímá data ze systému automatické analýzy objektů. Systém zpracovává všechny objekty odeslané společnosti Kaspersky. Systém poté určí pověst objektu a přidá data do antivirových databází. Pokud systém nedokáže určit reputaci objektu, dotazuje se analytiků virů ve společnosti Kaspersky.

Sandbox



Odborná analýza

Kaspersky Endpoint Security používá údaje o hrozbách přidávané analytiky virů společnosti Kaspersky. Pokud nelze reputaci objektu určit automaticky, analytikové virů jej vyhodnotí.

Kaspersky Endpoint Security zpracovává objekt ve virtuálním počítači. Kaspersky Sandbox analyzuje chování objektu a rozhodne o jeho reputaci. Tato technologie je k dispozici, pouze pokud používáte řešení Kaspersky Sandbox.



Cloud Sandbox

Kaspersky Endpoint Security kontroluje objekty v izolovaném prostředí poskytnutém společností Kaspersky. Technologie Cloud Sandbox je trvale povolena a je k dispozici všem uživatelům služby Kaspersky Security Network bez ohledu na typ licence, který používají. Pokud jste už nasadili řešení Endpoint Detection and Response, můžete povolit samostatné počítadlo hrozeb zjištěných technologií Cloud Sandbox.

Strom výběru

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

Strom výběru

Část	Součást
Základní ochrana před hrozbami 	**Ochrana před souborovými hrozbami** Součást Ochrana před souborovými hrozbami umožňuje zabránit infekci systému souborů počítače. Ve výchozím nastavení je součást Ochrana před souborovými hrozbami trvale umístěna v paměti RAM počítače a v reálném čase kontroluje všechny otevřené, uložené a spuštěné soubory. Tato součást kontroluje soubory na všech jednotkách počítače včetně připojených jednotek. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy. **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. **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 poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy. Ochrana před hrozbami v poště může kontrolovat příchozí i odchozí zprávy. Aplikace podporuje POP3, SMTP, IMAP a NNTP v následujících poštovních klientech: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Pokud chcete kontrolovat provoz v poštovních klientech Mozilla Thunderbird, MyOffice Mail a R7-Office Organizer, musíte přidat certifikát Kaspersky do úložiště certifikátů a vybrat vlastní úložiště certifikátů. Ochrana před hrozbami v poště nepodporuje jiné protokoly a poštovní klienty. Ochrana před hrozbami v poště nemusí být vždy schopna získat přístup ke zprávám na *úrovni protokolu* (například při použití řešení Microsoft Exchange). Z tohoto důvodu Ochrana před hrozbami pošty zahrnuje rozšíření pro Microsoft Office Outlook. Rozšíření umožňuje kontrolu zpráv na *úrovni poštovního klienta*. Rozšíření Ochrana před hrozbami v poště podporuje 32bitové verze aplikace Outlook 2010, 2013, 2016, 2019, 2021, 2024 a 365. V počítačích s architekturou ARM podporuje rozšíření Ochrana před hrozbami v poště 32bitové verze aplikace Outlook 2016, Outlook 2021, Outlook 2024 a Outlook 365 pro Arm64. **Ochrana před síťovými hrozbami** Součást *Ochrana před síťovými hrozbami* (také nazývaná Intrusion Detection System, IDS) monitoruje příchozí síťový provoz a sleduje aktivitu charakteristickou pro síťové útoky. Pokud aplikace 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. Seznam síťových útoků, které je součást Ochrana před síťovými hrozbami schopna zjistit, se aktualizuje při aktualizacích databází a modulů aplikace. **Brána firewall**

Součást 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*.

Ochrana před útoky BadUSB

Součást Ochrana před útoky BadUSB brání tomu, aby se infikovaná zařízení USB napodobující klávesnici připojila k počítači.

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.

Rozšířená ochrana před hrozbami



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 reputaci kontrolovaných webových adres a také informace o reputaci kategorii a reputaci kontrolovaných souborů .

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 je založeno na podpisech BSS a poskytuje aktivní ochranu počítače.

Součást Detekce chování navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

Anti-Cryptor

Součást Anti-Cryptor 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.

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.

Součást Prevence zneužití navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

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.

Modul pro nápravu

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

Kontrolní prvky zabezpečení



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.

Kontrola zařízení

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.

Kontrola webu

Součást 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 nebo zobrazí upozornění.

Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií sleduje a blokuje akce, které nejsou obvyklé pro počítače v podnikové síti. Adaptivní kontrola anomálií používá ke sledování netypického 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.

Kontrola protokolu

Kontrola protokolu monitoruje integritu chráněného prostředí na základě analýzy protokolu událostí systému Windows. Pokud aplikace zjistí známky netypického chování systému, informuje o tom správce, protože toto chování může znamenat pokus o kybernetický útok.

Monitorování integrity systému

Součást Monitorování integrity systému monitoruje změny v operačním systému, které mohou naznačovat narušení zabezpečení počítače. V případě zjištění takovýchto změn Kaspersky Endpoint Security vygeneruje odpovídající události a upozorní správce.

Úlohy



Kontrola malwaru

Aplikace Kaspersky Endpoint Security kontroluje počítač na přítomnost virů a dalších hrozeb. Kontrola malwaru pomůže vyloučit možnost šíření malwaru, který nebyl zjištěn součástmi ochrany, například v důsledku nízké úrovně zabezpečení.

Aktualizace databází a modulů aplikace

Aplikace Kaspersky Endpoint Security stahuje aktualizované databáze a moduly aplikace. Aktualizace chrání počítač před nejnovějšími viry a jinými hrozbami. Aplikace je ve výchozím nastavení aktualizována automaticky. V případě potřeby však můžete aktualizovat databáze a moduly aplikace ručně.

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.

Kontrola integrity aplikací

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.

Šifrování dat



Šifrování na úrovni souborů

Tato součást umožňuje vytvářet pravidla šifrování souborů. Můžete vybrat předdefinované složky pro šifrování, vybrat složku ručně nebo vybrat jednotlivé soubory podle přípony.

Úplné šifrování disku

Tato součást umožňuje šifrování pevného disku pomocí technologie Kaspersky Disk Encryption nebo BitLocker Drive Encryption.

Šifrování vyměnitelných jednotek

Tato součást umožňuje ochranu dat na vyměnitelných jednotkách. Můžete použít šifrování celého disku (FDE) nebo šifrování na úrovni souborů (FLE).

Detection and Response



Endpoint Detection and Response Optimum

Integrovaný agent pro řešení Kaspersky Endpoint Detection and Response Optimum (dále také „EDR Optimum"). *Kaspersky Endpoint Detection and Response* je řešením pro ochranu IT podnikové infrastruktury před pokročilými kybernetickými hrozbami. Funkce řešení kombinuje automatickou detekci hrozeb se schopností reagovat na tyto hrozby a čelit tak pokročilým útokům včetně nových exploitů, ransomwaru, bezsouborových útoků a metod využívajících legitimní systémové nástroje. Další informace o řešení najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum.

Endpoint Detection and Response Expert

Integrovaný agent pro řešení Kaspersky Endpoint Detection and Response Expert (dále také „EDR Expert"). EDR Expert nabízí více funkcí sledování hrozeb a reakce na ně než EDR Optimum. Další informace o tomto řešení najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

Endpoint Detection and Response Expert (on-premise) a **Network Detection and Response (KATA)**

Integrovaní agenti pro správu součástí Endpoint Detection and Response a Network Detection and Response, které jsou součástí řešení 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. Kaspersky Anti Targeted Attack Platform obsahuje tři funkční jednotky:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Všechny funkční jednotky nebo jednotlivé funkční jednotky můžete zakoupit samostatně. Podrobnosti o tomto řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

Sandbox

Integrovaný agent pro součást Sandbox. Součást *Sandbox* detekuje a automaticky blokuje pokročilé hrozby na počítačích. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Podrobnosti o tomto řešení najdete v nápovědě k součásti Kaspersky Sandbox a nápovědě k řešení Kaspersky Anti Targeted Attack Platform.

Managed Detection and Response

Integrovaný agent pro podporu provozu řešení Kaspersky Managed Detection and Response. Řešení *Kaspersky Managed Detection and Response (MDR)* automaticky detekuje a analyzuje bezpečnostní incidenty ve vaší infrastruktuře. K tomu používá MDR telemetrická data přijatá z koncových bodů a strojové učení. MDR zasílá údaje o incidentech odborníkům společnosti Kaspersky. Tito odborníci pak mohou incident zpracovat a například přidat nový záznam do antivirových databází. Alternativně mohou odborníci vydat doporučení ke zpracování incidentu a například navrhnout izolaci počítače od sítě. Podrobné informace o tom, jak řešení funguje, najdete v nápovědě k aplikaci Kaspersky Managed Detection and Response.

Režimy aplikace: Standardní, EDR Agent, Light Agent

Kaspersky Endpoint Security pro systém Windows je součástí mnoha řešení společnosti Kaspersky. V závislosti na řešení je třeba vybrat pro aplikaci režim.



Standardní režim

Toto je hlavní a výchozí režim aplikace. Aplikaci v tomto režimu můžete nainstalovat jako součást řešení Kaspersky EPP (Endpoint Protection Platform). Například aplikace Kaspersky Endpoint Security ve standardním režimu je součástí aplikace Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security poskytuje komplexní ochranu pracovních stanic a serverů před různými hrozbami, síťovými útoky a podvody. Ve standardním režimu jsou také k dispozici integrovaní agenti pro integraci s řešeními Kaspersky Detection and Response, včetně EDR, MDR, KUMA a dalších.



EDR Agent

Tento režim umožňuje nasadit řešení Kaspersky Detection and Response společně s řešeními EPP třetích stran. Mezi řešení Detection and Response patří Kaspersky Managed Detection and Response (MDR) a Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent také podporuje řešení Kaspersky SIEM, Kaspersky Unified Monitoring and Analysis Platform (KUMA).

V tomto režimu nejsou k dispozici standardní součásti ochrany, jako je Ochrana před souborovými hrozbami nebo Ochrana před webovými hrozbami. Standardní ochranu počítače poskytuje řešení EPP třetí strany. EDR Agent nepřetržitě monitoruje procesy spuštěné v těchto počítačích, otevřená síťová připojení a upravované soubory a spolupracuje s řešeními Detection and Response.



Light Agent

Tento režim se používá k ochraně virtuálních prostředí. Kaspersky Endpoint Security v režimu Light Agent je součástí řešení Kaspersky Hybrid Cloud Security. Light Agent chrání virtuální počítače s hostovanými operačními systémy pro pracovní stanice a servery. V tomto režimu jsou k dispozici stejné součásti ochrany a kontroly jako ve standardním režimu. Rozdíl je v tom, že objekty jsou kontrolovány na výskyt virů a jiného malwaru pomocí zvláštní součásti-řešení nainstalované na samostatném virtuálním počítači, SVM (Secure Virtual Machine). Light Agent tedy místo prostředků virtuálního počítače používá k zajištění zabezpečení infrastruktury prostředky SVM.

Distribuční sada

Distribuční sada obsahuje následující distribuční balíčky:

- **AES256**

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

- **AES56**

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

  Distribuční balíčky AES256 a AES56 nejsou určeny pro instalaci do počítačů s architekturou ARM.

- **Arm64**

  Tento distribuční balíček je určen k instalaci na počítače s architekturou ARM.

  Distribuční balíček Arm64 není určen pro instalaci do počítačů s operačními systémy Windows x86/x64 nebo operačními systémy Windows pro servery.

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 pro modul plug-in pro správu aplikací v konzole pro správu aplikace Kaspersky Security Center.
`bases.cab`	Soubory aktualizačního balíčku používané během instalace.
`cleaner_v2.cab` `cleanerapi_v2.cab`	Soubory k odebrání nekompatibilního softwaru.
`incompatible.txt`	Soubor obsahující seznam softwaru, který může způsobit problémy s kompatibilitou s aplikací Kaspersky Endpoint Security. Společnost Kaspersky nezaručuje kompatibilitu aplikace Kaspersky Endpoint Security se softwarem ze seznamu.
`ksn_<language ID>.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.
`kes.cab`	Soubory pro grafické rozhraní aplikace.
`aes256.cab` / `aes56.cab`	Soubory pro šifrovací algoritmus AES (není součástí distribučního balíčku Arm64).
`package.kcat`	Soubor s podpisy distribuční sady aplikace. Digitální podpis zaručuje pravost a integritu distribučního balíčku aplikace.

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 instrukcí SSE2 (kromě Arm)
- RAM:
  - Pracovní stanice (x86): 1 GB
  - Pracovní stanice (x64): 2 GB
  - Server: 2 GB
  - Server pro instalaci aplikace s integrovaným agentem pro integraci s řešením Kaspersky Anti Targeted Attack Platform: 8 GB
- Microsoft .NET Framework 4 nebo novější

Minimální obecné požadavky pro počítače s architekturou ARM:

- 2 GB volného místa na pevném disku
- CPU: 1 GHz, architektura Armv8.1
- RAM: 4 GB
- Microsoft .NET Framework 4.8 nebo novější

K instalaci aplikace potřebujete práva správce v počítači.

Pracovní stanice

Podporované operační systémy pro pracovní stanice:

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

Operační systémy Windows počínaje verzí 11 24H2 podporují technologii UDP Receive Segment Coalescing Offload (URO). Tato technologie je ve výchozím nastavení povolena, pokud je v počítači nainstalována kompatibilní síťová karta a ovladače. Zakázání URO v počítači uživatele může výrazně snížit výkon aplikace.

Aby aplikace Kaspersky Endpoint Security fungovala správně, musí být v počítači uživatele spuštěna služba Windows Security Center (wscsvc).

Kaspersky Endpoint Security nelze nainstalovat na Microsoft Windows 7 bez nainstalovaných aktualizací operačního systému: KB4490628 (12. března 2019) a KB4474419 (23. září 2019). Podrobné informace naleznete ve znalostní bázi technické podpory.

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

Podrobnosti o podpoře operačního systému Microsoft Windows 11 najdete ve znalostní bázi technické podpory.

Servery

Kaspersky Endpoint Security podporuje základní součásti aplikace v počítačích s operačním systémem Windows pro servery. Na serverech a v clusterech vaší organizace můžete používat aplikaci Kaspersky Endpoint Security pro systém Windows místo Kaspersky Security for Windows Server (Cluster Mode). Aplikace rovněž podporuje Server Core Mode (viz známé problémy).

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;
- Windows Web Server 2008 R2 Service Pack 1;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (včetně režimu Server Core)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2016 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (včetně režimu Server Core);
- Windows Server 2025 Standard / Datacenter.

Kaspersky Endpoint Security nelze nainstalovat na Microsoft Windows Server 2008 R2 bez nainstalovaných aktualizací operačního systému: KB4490628 (12. března 2019) a KB4474419 (23. září 2019).

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

Podrobnosti o podpoře operačního systému Microsoft Windows Server 2022 najdete ve znalostní bázi technické podpory.

Nepodporované operační systémy pro servery:

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

Virtuální platformy

Virtuální platformy podporované pro provoz aplikací ve standardním režimu:

- VMware Workstation Pro 17.6.4
- VMware ESXi 8.0, aktualizace 3g
- Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4

Aplikace podporuje virtuální stroje se systémem Windows 11 Pro Arm64 vytvořené pomocí Hyper-V.

Virtuální počítače pro instalaci režimu Light Agent

Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent na virtuálních počítačích s architekturou ARM není podporována.

Systém BIOS na virtuálních počítačích musí podporovat specifikaci SMBIOS verze 2.1 nebo novější.

Na virtuálních počítačích musí být nainstalovány následující balíčky a nástroje:

- Při používání Microsoft Hyper-V – balíček Integration Services.
- Při používání VMware vSphere – balíček VMware Tools.
- Při používání XenServer – balíček XenTools.
- Při používání HUAWEI FusionSphere – balíček HUAWEI Tools.
- Při používání hypervizorů založených na KVM – QEMU Guest Agent.

Požadavky na virtuální infrastrukturu pro spuštění aplikace v režimu Light Agent najdete v nápovědě k součásti Kaspersky Security for Virtualization Light Agent.

Aby aplikace fungovala správně, používejte virtualizované síťové rozhraní s šířkou pásma alespoň 100 Mbit/s.

Terminálové servery

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
- Microsoft Remote Desktop Services na základě Windows Server 2022
- Microsoft Remote Desktop Services na základě Windows Server 2025
- Citrix RDSH z Citrix Virtual Apps and Desktops 7 2507 LTSR

Podpora aplikace Kaspersky Security Center

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

- Kaspersky Security Center 14
- Kaspersky Security Center 14.1
- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2

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).

Počínaje aplikací Kaspersky Endpoint Security 12.8 pro systém Windows můžete v instalačním balíčku nakonfigurovat různé sady součástí pro různé typy operačního systému. To znamená, že aplikaci můžete nasadit na pracovní stanice a servery pomocí instalačního balíčku.

Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent na virtuálních počítačích s architekturou ARM není podporována.

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Pracovní stanice	Pracovní stanice s architekturou ARM	Server	Režim Server Core
Rozšířená ochrana před hrozbami				
Kaspersky Security Network	✓	✓	✓	✓
Detekce chování	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓
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 protokolu	–	–	✓	–
Kontrola aplikací	✓	✓	✓	✓
Kontrola zařízení	✓	✓	✓	✓
Kontrola webu	✓	✓	✓	–
Adaptivní kontrola anomálií	✓	✓	–	–
Monitorování integrity systému	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Šifrování dat				
Kaspersky Disk Encryption	✓	–	–	–
BitLocker Drive Encryption	✓	✓	✓	✓
Šifrování na úrovni souborů	✓	–	–	–
Šifrování vyměnitelných jednotek	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert	✓	–	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
Integrace KUMA	✓	✓	✓	✓

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:

- 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. *Kaspersky Security Center Cloud Console* 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 nápovědě ke cloudové konzole aplikace Kaspersky Security Center.

Kaspersky Endpoint Security je součástí řešení Kaspersky Next Pro View. Další informace o dostupných funkcích aplikace, když funguje jako součást tohoto řešení, najdete v nápovědě k řešení Kaspersky Next.

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Kaspersky Security Center		Kaspersky Security Center
	Konzola pro správu	Webová konzola	Cloudová konzola
Rozšířená ochrana před hrozbami			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Detekce chování	✓	✓	✓
Anti-Cryptor			
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 protokolu	✓	✓	✓
Kontrola aplikací	✓	✓	✓
Kontrola zařízení	✓	✓	✓
Kontrola webu	✓	✓	✓
Adaptivní kontrola anomálií	✓	✓	✓
Monitorování integrity systému	✓	✓	✓
Cloud Discovery	–	–	✓
Šifrování dat			
Kaspersky Disk Encryption	✓	✓	–
BitLocker Drive Encryption	✓	✓	✓
Šifrování na úrovni souborů	✓	✓	–
Šifrování vyměnitelných jednotek	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
Integrace KUMA	✓	✓	✓
Úlohy			
Přidání klíče	✓	✓	✓
Změna součástí aplikace	✓	✓	✓
Inventarizace	✓	✓	✓

Aktualizovat	✓	✓	✓
Vrácení aktualizace zpět	✓	✓	✓
Kontrola malwaru	✓	✓	✓
Kontrola integrity aplikací	✓	✓	–
Výmaz dat	✓	✓	✓
Správa účtů ověřovacího agenta (Kaspersky Disk Encryption)	✓	✓	–
Kontrola IOC (EDR)	–	✓	✓
Přesunout soubor do karantény (EDR)	–	✓	✓
Načíst soubor (EDR)	–	✓	✓
Odstranit soubor (EDR)	–	✓	✓
Spustit proces (EDR)	–	✓	✓
Ukončit proces (EDR)	–	✓	✓

Kompatibilita s jinými aplikacemi

Kaspersky Endpoint Security je nekompatibilní s některými aplikacemi Kaspersky a také s některými aplikacemi třetích stran. Před instalací, aktualizací verze aplikace a změnou součástí aplikace proto aplikace Kaspersky Endpoint Security zkontroluje počítač, aby zjistila, zda v něm nějaké takové aplikace nejsou.

Kompatibilita s aplikacemi třetích stran

Kaspersky Endpoint Security je nekompatibilní s aplikacemi, které jsou součástí systémů ochrany koncových bodů třetích stran (Endpoint Protection Platform, EPP). Kaspersky Endpoint Security může také narazit na problémy s kompatibilitou s jinými aplikacemi. Pro určení kompatibility aplikace Kaspersky Endpoint Security konzulutuje seznam softwaru připravený společností Kaspersky. Tento seznam je obsažen v souboru incompatible.txt. Tento soubor je součástí distribučního balíčku.

Společnost Kaspersky nezaručuje kompatibilitu aplikace Kaspersky Endpoint Security se softwarem ze seznamu. Pokud je nalezena aplikace ze seznamu, instalační program zastaví nasazování aplikace Kaspersky Endpoint Security. Instalační program může automaticky odstranit některé aplikace ze seznamu. Pokud jste ochotni ignorovat rizika a chcete nainstalovat Kaspersky Endpoint Security a software ze seznamu na stejný počítač, můžete kontrolu počítače přeskočit (viz pokyny níže).

STAŽENÍ NEKOMPATIBILNÍHO SOUBORU .TXT

Kompatibilita s aplikacemi Kaspersky

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

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security
- Kaspersky Anti-Virus
- Kaspersky Total Security
- Kaspersky Safe Kids
- Kaspersky Free
- Kaspersky Anti-Ransomware Tool
- Endpoint Sensor jako součást řešení Kaspersky Anti Targeted Attack Platform a Kaspersky Endpoint Detection and Response.
- Kaspersky Endpoint Agent jako součást řešení Detection and Response od společnosti Kaspersky.

> Společnost Kaspersky všechna řešení Detection and Response převádí tak, aby fungovala s integrovaným agentem Kaspersky Endpoint Security namísto aplikace Kaspersky Endpoint Agent. Počínaje verzí 12.1 aplikace podporuje všechna řešení Detection and Response.

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

  > Od aplikace Kaspersky Endpoint Security 12.0 můžete migrovat z aplikace Kaspersky Security for Windows Server na aplikaci Kaspersky Endpoint Security pro systém Windows a používat stejné řešení k ochraně pracovních stanic i serverů.

- 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.

Přeskočení kontroly softwaru, který může způsobit problémy s kompatibilitou

Pokud aplikace Kaspersky Endpoint Security detekuje software ze seznamu incompatible.txt, instalace aplikace bude ukončena. Chcete-li pokračovat v instalaci, musíte tuto aplikaci odebrat. Pokud však dodavatel softwaru třetí strany ve své dokumentaci uvedl, že je jeho software kompatibilní s platformami Endpoint Protection Platform (EPP), můžete do počítače obsahujícího aplikaci od tohoto dodavatele nainstalovat aplikaci Kaspersky Endpoint Security. Například poskytovatel řešení Endpoint Detection and Response (EDR) může deklarovat svoji kompatibilitu se systémy EPP třetích stran. V takovém případě je třeba zahájit instalaci aplikace Kaspersky Endpoint Security bez spouštění kontroly nainstalovaného softwaru. To provedete tak, že instalačnímu programu předáte následující parametry:

- `SKIPPRODUCTCHECK=1`. Zakáže kontrolu nainstalovaného softwaru. Seznam softwaru, který může způsobovat problémy s kompatibilitou, je k dispozici v souboru incompatible.txt, který je součástí distribuční sady. Pokud není u tohoto parametru nastavena žádná hodnota a je zjištěn software ze seznamu, instalace aplikace Kaspersky Endpoint Security bude ukončena.
- `SKIPPRODUCTUNINSTALL=1`. Zakáže automatické odstranění zjištěného softwaru ze seznamu incompatible.txt. Pokud není u tohoto parametru nastavena žádná hodnota, aplikace Kaspersky Endpoint Security se pokusí software, který může způsobovat problémy s kompatibilitou, odebrat.
- `CLEANERSIGNCHECK=0`. Zakázání ověřování digitálního podpisu aplikací nalezených kontrolou. Pokud tento parametr není nastaven, ověřování digitálních podpisů je při nasazování aplikace prostřednictvím Kaspersky Security Center zakázáno. Když je aplikace instalována lokálně, ověřování digitálního podpisu je ve výchozím nastavení povoleno.

Při místní instalaci aplikace můžete předat parametry v příkazovém řádku.

Pokud jste během procesu instalace přeskočili kontrolu softwaru, který může způsobovat problémy s kompatibilitou, Kaspersky Endpoint Security může tuto kontrolu provést znovu, když se změní součásti aplikace. Chcete-li kontrolu nainstalovaného softwaru přeskočit, musíte nakonfigurovat úlohu *Změna součástí aplikace*.

Příklad:

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

Chcete-li aplikaci Kaspersky Endpoint Security nainstalovat vzdáleně, musíte přidat příslušné parametry do souboru pro generování instalačního balíčku s názvem `kes_win.kud` v části `[Setup]` (viz níže). Soubor `kes_win.kud` je součástí distribučního balíčku.

kes_win.kud

```
[Setup]

UseWrapper=1

ExecutableRelPath=EXEC

Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0

Executable=setup_kes.exe

RebootDelegated = 1

RebootAllowed=1

ConfigFile=installer.ini

RelPathsToExclude=klcfginst.msi
```

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,
- vzdáleně prostřednictvím editoru správy zásad skupiny v systému Microsoft Windows (další podrobnosti najdete na webu 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.
4. Nastavení přijatá z konfiguračního souboru (install.cfg).

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

Při instalaci aplikace Kaspersky Endpoint Security může operační systém zobrazovat své vlastní zprávy. Při instalaci aplikace může být rovněž přerušeno síťové a internetové připojení.

Při instalaci, aktualizaci nebo odinstalaci aplikace Kaspersky Endpoint Security může dojít k chybám. Další informace o řešení těchto chyb naleznete ve znalostní bázi technické podpory .

Nasazení prostřednictvím aplikace Kaspersky Security Center

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. Před instalací aplikace se musíte ujistit, že je v počítači nainstalována aplikace Kaspersky Security Center Network Agent. Součást *Network Agent* usnadňuje interakci mezi serverem pro správu a klientským počítačem.

Kaspersky Security Center 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 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 .

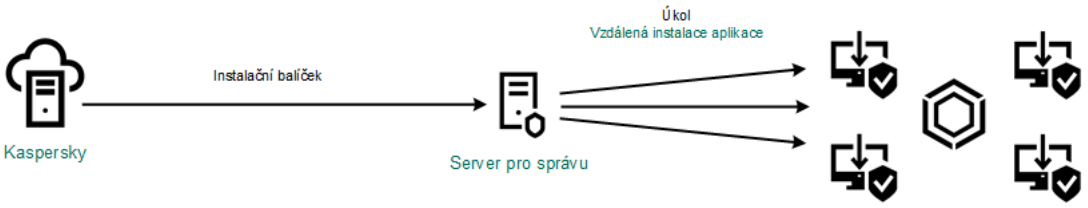
Standardní instalace aplikace

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 *Install application remotely* serveru pro správu aplikace Kaspersky Security Center.



Nasazení aplikace Kaspersky Endpoint Security

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

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Advanced** → **Remote installation**.
3. Klikněte na odkaz **Deploy installation package on managed devices (workstations)**.

Spustí se průvodce Protection 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.

Krok 2. Výběr zdroje instalačního balíčku

Vyberte zdroj **Deploy Kaspersky Security Center package**.

Step 3. 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 4. Definování nastavení úlohy vzdálené instalace

Nakonfigurujte následující další nastavení aplikace:

- **Force installation package download**. Vyberte způsob instalace aplikace:
  - **Using Network Agent**. Za doručení instalačního balíčku aplikace Kaspersky Endpoint Security do klientských počítačů je odpovědná součást Network Agent. Pokud součást Network Agent není nainstalována, úloha skončí chybou. V takovém případě přidejte instalační balíček součásti Network Agent do úlohy *Install application remotely* a povolte doručování souborů prostřednictvím prostředků operačního systému. Poté bude součást Network Agent nainstalována pomocí prostředků operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
  - **Using operating system resources through distribution points**. 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.

- **Using operating system resources through Administration Server**. 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.

- **Behavior for devices managed through other Administration Servers**. 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 re-install application if it is already installed**. Zrušte zaškrtnutí tohoto políčka, pokud chcete například nainstalovat starší verzi aplikace.

- **Assign Network Agent installation in 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 5. 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 *Add key*.

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.

Krok 8. 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 9. Zahájení instalace

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. 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 **Discovery & deployment → Deployment & assignment → Protection deployment wizard**.

Spustí se průvodce Protection 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 *Add key*.

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:

- **Force installation package download**. Vyberte způsob instalace aplikace:
  - **Using Network Agent**. Za doručení instalačního balíčku aplikace Kaspersky Endpoint Security do klientských počítačů je odpovědná součást Network Agent. Pokud součást Network Agent není nainstalována, úloha skončí chybou. V takovém případě přidejte instalační balíček součásti Network Agent do úlohy *Install application remotely* a povolte doručování souborů prostřednictvím prostředků operačního systému. Poté bude součást Network Agent nainstalována pomocí prostředků operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.
  - **Using operating system resources through distribution points**. 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.
  - **Using operating system resources through Administration Server**. 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 re-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 **Run the task after the wizard finishes**. 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 **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.
   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.
2. Klikněte na tlačítko **Create installation package**.

Spustí se průvodce novým balíčkem. Postupujte podle pokynů průvodce.

Krok 1. Výběr typu instalačního balíčku

Vyberte možnost **Create an installation package for a Kaspersky application**.

Krok 2. Definice názvu instalačního balíčku

Zadejte název instalačního balíčku, například *Kaspersky Endpoint Security pro systém Windows 14.0*.

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 **Copy updates from repository to installation package**.

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.

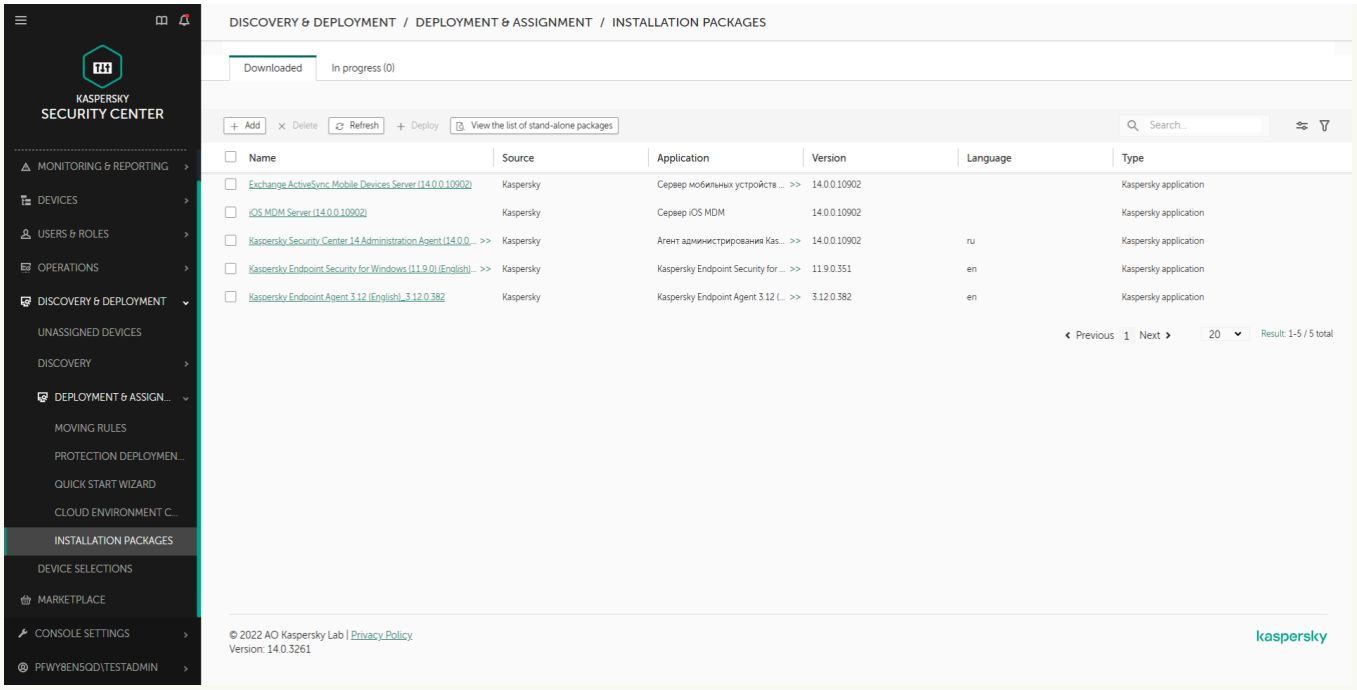
V nastavení instalačního balíčku můžete vybrat součásti aplikace pro různé typy operačních systémů. To znamená, že instalační balíček obsahuje dvě sady součástí: pro pracovní stanice a pro servery. Před nasazením instalačního balíčku instalační program zjistí typ operačního systému a nainstaluje pouze ty součásti aplikace, které jste vybrali pro daný typ operačního systému. Stejný instalační balíček tak můžete použít pro pracovní stanice i servery.

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 konzoly vyberte možnosti **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.
   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce novým balíčkem. Postupujte podle pokynů průvodce.



Seznam instalačních balíčků

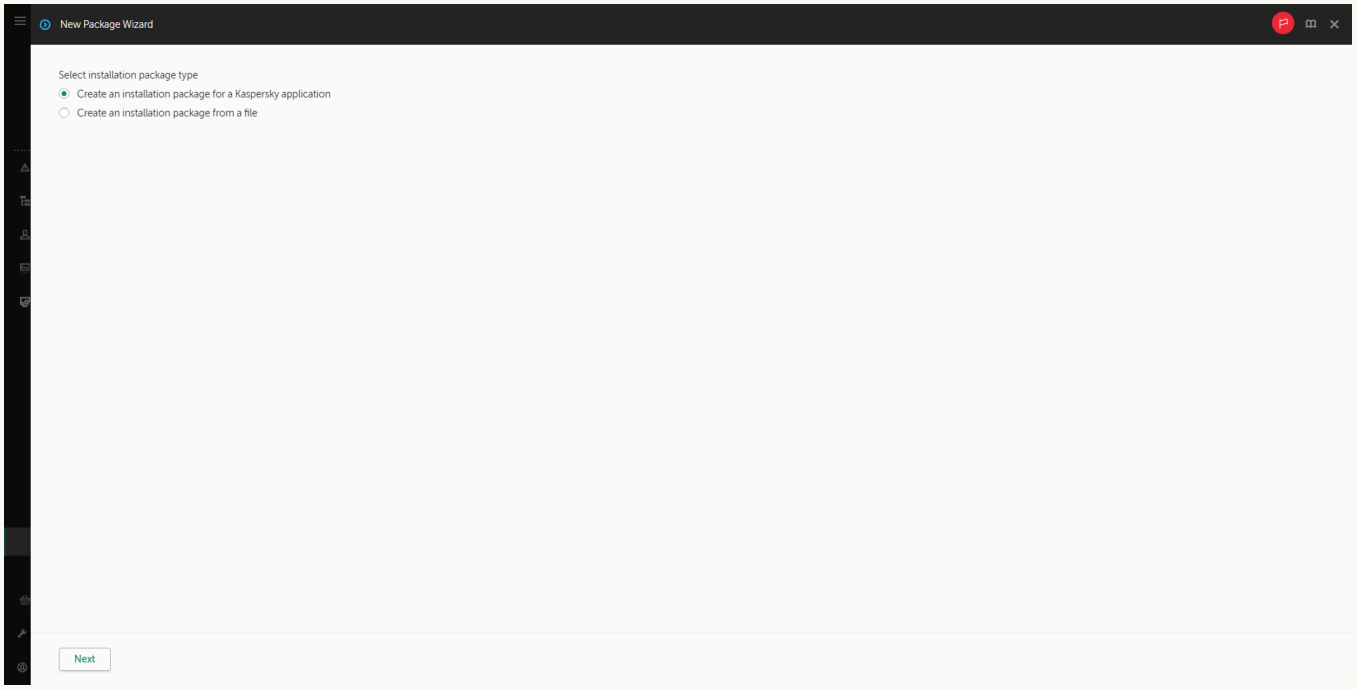
Krok 1. Výběr typu instalačního balíčku

Vyberte možnost **Create an installation package for a Kaspersky application**.

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.

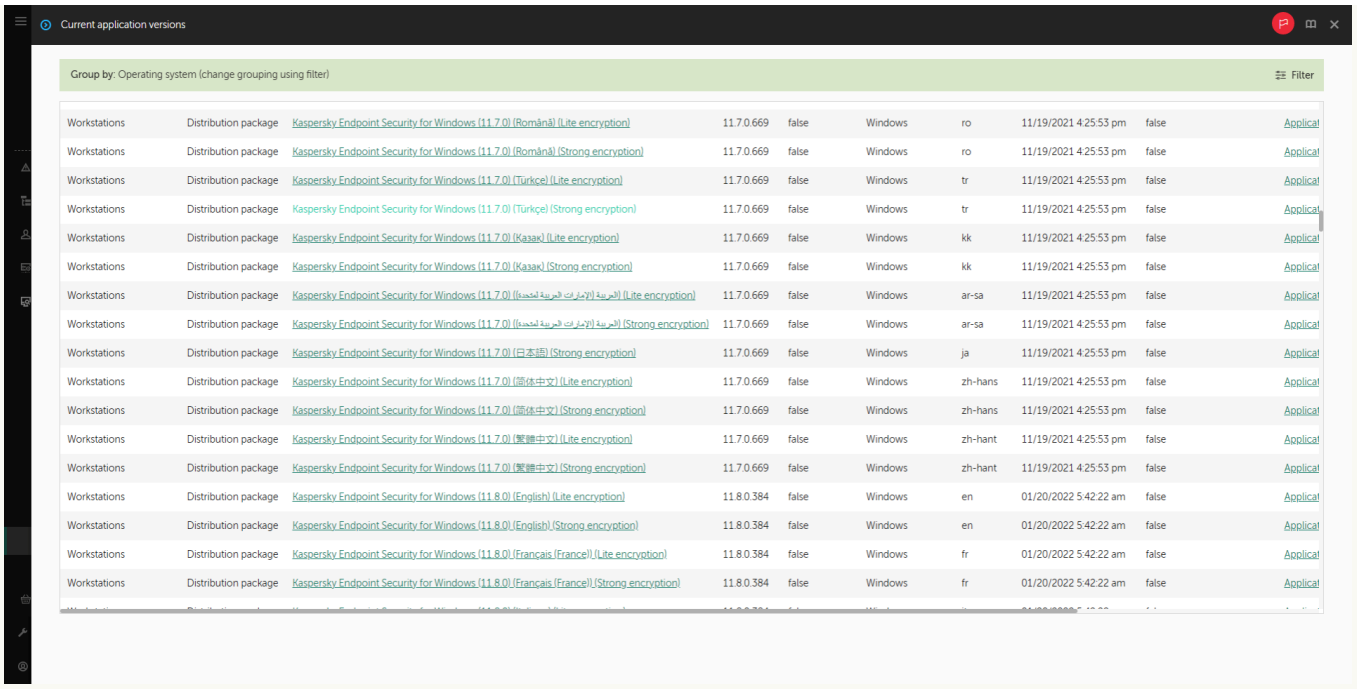
Vytvoření instalačního balíčku pro aplikaci Kaspersky Endpoint Security ze souboru je k dispozici pouze ve webové konzole aplikace Kaspersky Security Center.



Typy instalačních balíčků

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.

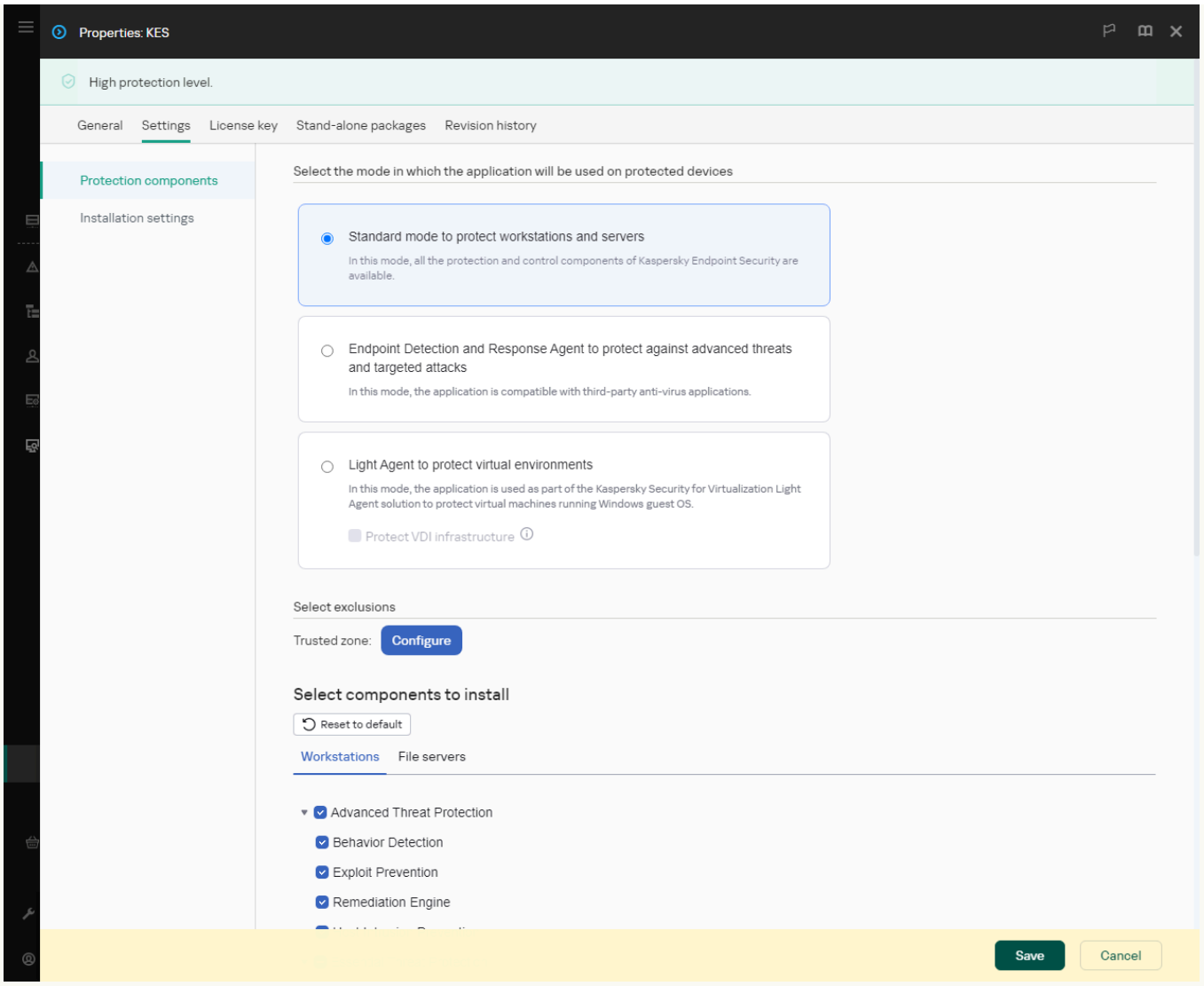


Seznam instalačních balíčků na serverech Kaspersky

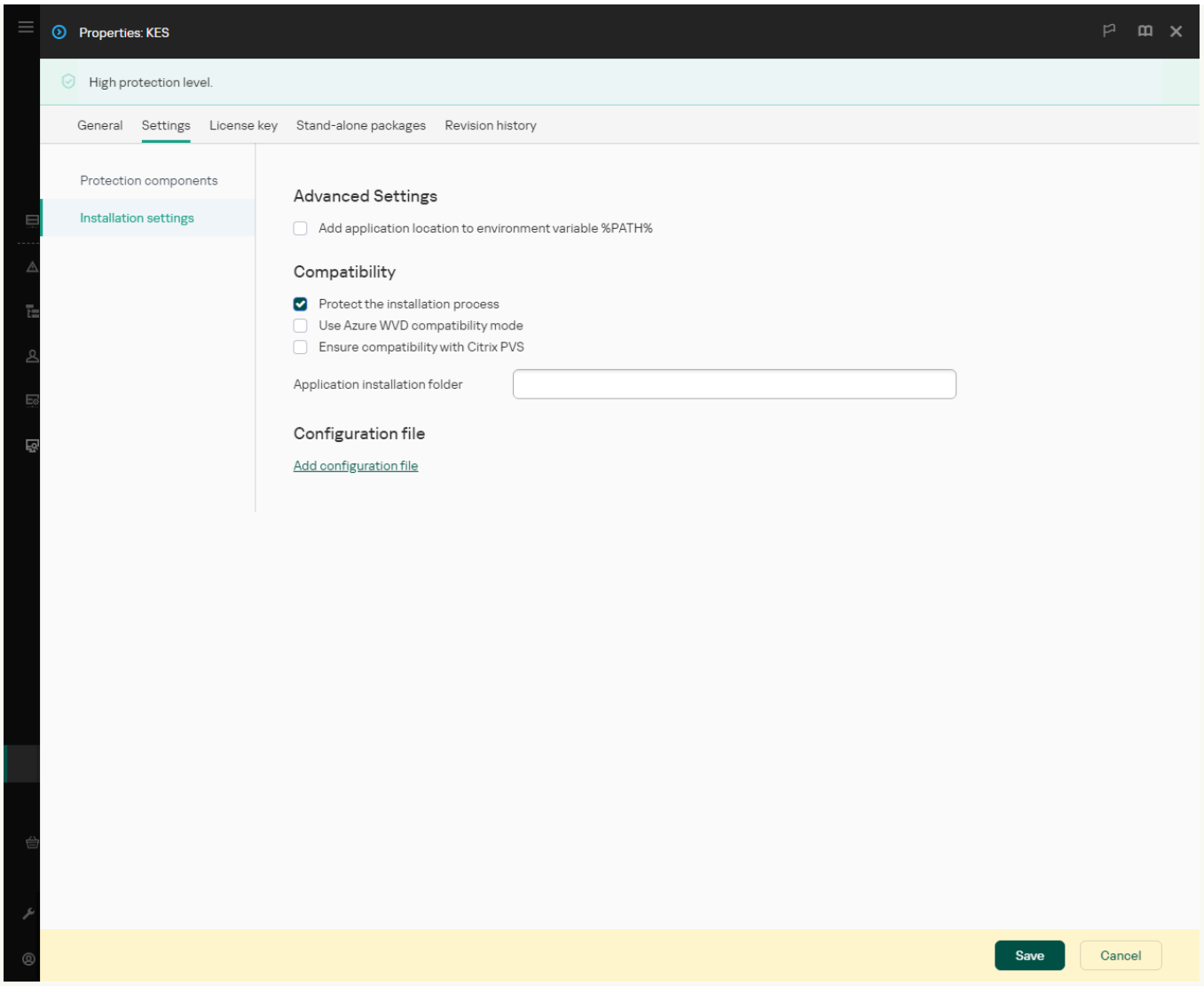
Vytvoří se instalační balíček a bude přidán do aplikace Kaspersky Security Center. Pomocí instalačního balíčku můžete nainstalovat aplikaci Kaspersky Endpoint Security do počítačů v podnikové síti nebo aktualizovat verzi aplikace.

V nastavení instalačního balíčku můžete vybrat součásti aplikace pro různé typy operačních systémů. To znamená, že instalační balíček obsahuje dvě sady součástí: pro pracovní stanice a pro servery. Před nasazením instalačního balíčku instalační program zjistí typ operačního systému a nainstaluje pouze ty součásti aplikace, které jste vybrali pro daný typ operačního systému. Stejný instalační balíček tak můžete použít pro pracovní stanice i servery.

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.



Součásti obsažené v instalačním balíčku



Nastavení instalace instalačního balíčku

Nastavení instalačního balíčku

Část	Popis
Součásti ochrany	**Standardní režim**. Výchozí konfigurace. Tato konfigurace vám umožňuje používat všechny součásti aplikace, včetně součástí, které poskytují podporu pro řešení Detection and Response. Tato konfigurace se používá pro komplexní ochranu počítače před různými hrozbami, síťovými útoky a podvody. **Endpoint Detection and Response Agent**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran. **Light Agent na ochranu virtuálních prostředí**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Chránit infrastrukturu VDI** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.
Výjimky	Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware. Důvěryhodnou zónu můžete nakonfigurovat také později ve vlastnostech zásad: výjimky z kontroly a důvěryhodné aplikace.
Výběr součástí k instalaci	V této části můžete vybrat součásti aplikace, které budou k dispozici. Později můžete změnit sadu součástí aplikace pomocí úlohy *Změna součástí aplikace*.

Pro pracovní stanici a servery můžete vytvořit samostatné kombinace součástí. Před nasazením instalačního balíčku instalační program zjistí typ operačního systému a nainstaluje pouze ty součásti aplikace, které jste vybrali pro daný typ operačního systému. Stejný instalační balíček tak můžete použít pro pracovní stanice i servery.

Sada dostupných součástí závisí na konfiguraci aplikace:

Standardní režim

Součást Ochrana před útoky BadUSB, součást Detection and Response a součásti šifrování dat nejsou ve výchozím nastavení nainstalovány. Tyto součásti lze přidat v nastaveních instalačního balíčku.

Endpoint Detection and Response Agent

V této konfiguraci jsou k dispozici pouze integrovaní agenti pro řešení Kaspersky Detection and Response.

Light Agent na ochranu virtuálních prostředí

V této konfiguraci můžete použít téměř všechny součásti aplikace, které jsou k dispozici v konfiguraci **Standardní režim**, s výjimkou součástí Šifrování dat a Adaptivní kontrola anomálií.

License key

V této části můžete aplikaci aktivovat. Pro aktivaci aplikace musíte vybrat licenční klíč. Než to uděláte, musíte přidat klíč na server pro správu. Podrobnosti o přidání klíčů na server pro správu aplikace Kaspersky Security Center najdete v nápovědě k aplikaci Kaspersky Security Center.

Incompatible applications

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.

Installation settings

Přidejte cestu k souboru avp.com do systémové proměnné %PATH%. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku.

Protect the installation process. 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 Windows Remote Desktop), doporučujeme ochranu instalace vypnout.

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

Použít režim kompatibility Azure WVD. Tato funkce zajišťuje správné zobrazení stavu virtuálního počítače Azure v konzole Kaspersky Anti Targeted Attack Platform. Pro sledování výkonu počítače odesílá Kaspersky Endpoint Security telemetrii na servery KATA. Telemetrie zahrnuje ID počítače (Sensor ID). Režim kompatibility Azure WVD umožňuje těmto virtuálním počítačům přiřadit trvalé jedinečné Sensor ID. Pokud je režim kompatibility vypnutý, Sensor ID se může po restartování počítače změnit kvůli tomu, jak fungují virtuální počítače Azure. To může způsobit, že se na konzole objeví duplikáty virtuálních počítačů.

Application installation folder. Můžete změnit cestu instalace aplikace Kaspersky Endpoint Security v klientském počítači. Ve výchozím nastavení je aplikace nainstalována do složky `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.0`.

Configuration file. Instalace aplikace s předdefinovaným nastavením. K tomu musíte 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 *Download updates to the Administration Server repository* 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. 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. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole vyberte možnosti **Advanced** → **Remote installation** → složku **Installation packages**.
   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.
3. Otevřete vlastnosti instalačního balíčku.
4. V části **General** klikněte na tlačítko **Update databases**.

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 konzoly vyberte možnosti **Discovery & deployment** → **Deployment & 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 **General information** klikněte na odkaz **Update databases**.

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 *Install application remotely* je určena pro vzdálenou instalaci aplikace Kaspersky Endpoint Security. Úloha *Install application remotely* 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. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve stromu konzoly vyberte možnost **Tasks**.

   Otevře se seznam úloh.

3. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte **Kaspersky Security Center Administration Server** → **Install application remotely**.

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:

- **Force installation package download**. Vyberte způsob instalace aplikace:

  - **Using Network Agent**. Za doručení instalačního balíčku aplikace Kaspersky Endpoint Security do klientských počítačů je odpovědná součást Network Agent. Pokud součást Network Agent není nainstalována, úloha skončí chybou. V takovém případě přidejte instalační balíček součásti Network Agent do úlohy *Install application remotely* a povolte doručování souborů prostřednictvím prostředků operačního systému. Poté bude součást Network Agent nainstalována pomocí prostředků operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.

  - **Using operating system resources through distribution points**. 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.

  - **Using operating system resources through Administration Server**. 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.

- **Behavior for devices managed through other Administration Servers**. 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 re-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 14.0*.

Krok 10. Vytvoření úloh po dokončení

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. 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 konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Security Center**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Install application remotely**.

3. V poli **Task name** zadejte krátký popis, například *Instalace aplikace Kaspersky Endpoint Security pro správce*.

4. V bloku **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 instalační balíček:

1. Vyberte instalační balíček aplikace Kaspersky Endpoint Security pro systém Windows (14.0).

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 bloku **Force installation package download** vyberte způsob instalace aplikace:

   - **Using Network Agent**. Za doručení instalačního balíčku aplikace Kaspersky Endpoint Security do klientských počítačů je odpovědná součást Network Agent. Pokud součást Network Agent není nainstalována, úloha skončí chybou. V takovém případě přidejte instalační balíček součásti Network Agent do úlohy *Install application remotely* a povolte doručování souborů prostřednictvím prostředků operačního systému. Poté bude součást Network Agent nainstalována pomocí prostředků operačního systému. Poté je nainstalována aplikace Kaspersky Endpoint Security pomocí nástrojů součásti Network Agent.

   - **Using operating system resources through distribution points**. 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.

   - **Using operating system resources through Administration Server**. 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 concurrent 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 **Maximum 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 re-install application if it is already installed**. Umožňuje například nainstalovat některou z předchozích verzí aplikace.

7. V případě potřeby zrušte zaškrtnutí políčka **Verify operating system type before downloading**. 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 **Prompt users to close 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 bloku **Behavior for devices managed through other Administration Servers** 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 **Finish** 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. Ujistěte se, že uživatelský účet, pod kterým spouštíte průvodce nastavením, je ve skupině správců.

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.

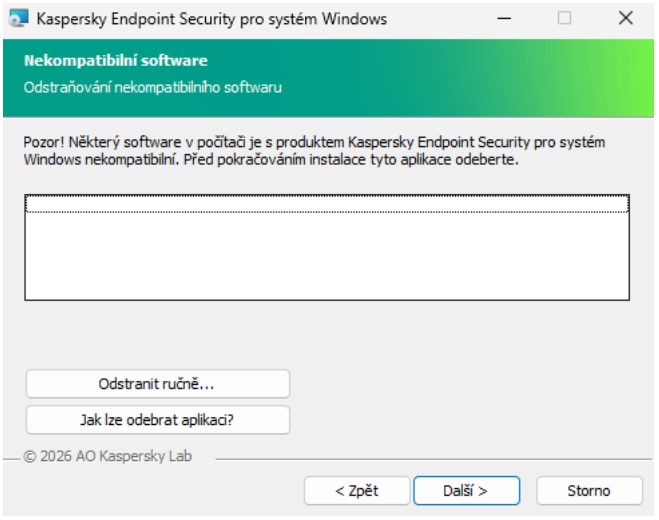
Spustí se Průvodce instalací.

Příprava na instalaci

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

- Přítomnost softwaru, se kterým může mít Kaspersky Endpoint Security problémy s kompatibilitou (seznam softwaru je k dispozici v souboru incompatible.txt, který je součástí distribuční sady).
- Zda jsou či nejsou splněny požadavky na hardware a software.
- Zda je přítomen Microsoft .NET Framework.
- Zda uživatel má či nemá práva k instalaci softwarového produktu.

Pokud jakýkoli z předchozích požadavků není splněn, na obrazovce se objeví příslušné upozornění. Například oznámení o nekompatibilním softwaru (viz obrázek níže).



Odstraňování nekompatibilního softwaru

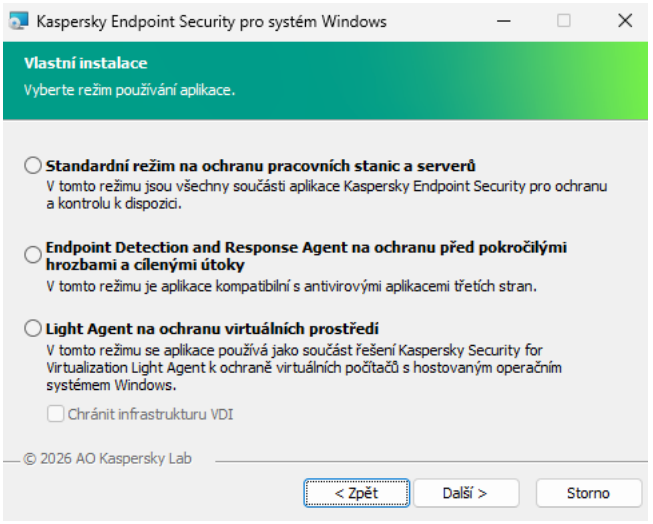
Jestliže počítač uvedené požadavky splňuje, průvodce instalací se pokusí najít aplikace společnosti Kaspersky, které by mohly způsobit konflikty při současném použití s instalovanou aplikací. Při nalezení takových aplikací budete vyzváni k jejich ručnímu odebrání.

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 14.0 pro systém Windows a předchozí verze aplikace je automaticky odebrána. To se týká následujících verzí aplikace:

- Kaspersky Endpoint Security 12.1 pro systém Windows (sestavení 12.1.0.506)
- Kaspersky Endpoint Security 12.2 pro systém Windows (sestavení 12.2.0.462)
- Kaspersky Endpoint Security 12.3 pro systém Windows (sestavení 12.3.0.493)
- Kaspersky Endpoint Security 12.4 pro systém Windows (sestavení 12.4.0.467)
- Kaspersky Endpoint Security 12.5 pro systém Windows (sestavení 12.5.0.539)
- Kaspersky Endpoint Security 12.6 pro systém Windows (sestavení 12.6.0.438)

- Kaspersky Endpoint Security 12.7 pro systém Windows (sestavení 12.7.0.533)
- Kaspersky Endpoint Security 12.8 pro systém Windows (sestavení 12.8.0.505)
- Kaspersky Endpoint Security 12.9 pro systém Windows (sestavení 12.9.0.384)
- Kaspersky Endpoint Security 12.10 pro systém Windows (sestavení 12.10.0.466)
- Kaspersky Endpoint Security 12.11 pro systém Windows (sestavení 12.11.0.637)
- Kaspersky Endpoint Security 12.12 pro systém Windows (sestavení 12.12.0.522)

Konfigurace aplikace Kaspersky Endpoint Security



Výběr konfigurace aplikace

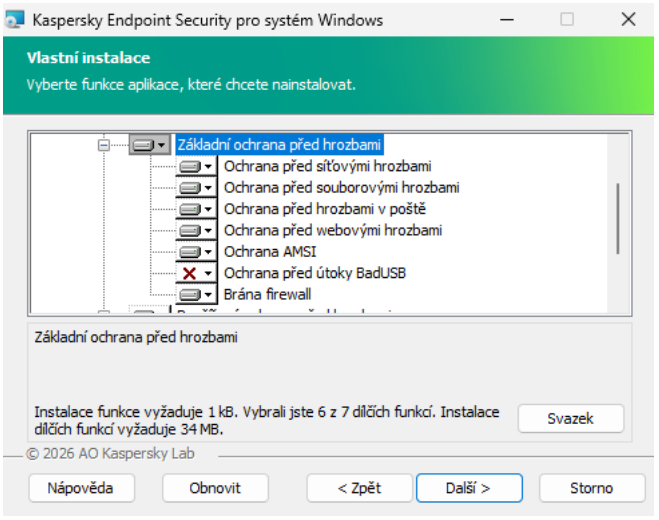
Standardní režim. Výchozí konfigurace. Tato konfigurace vám umožňuje používat všechny součásti aplikace, včetně součástí, které poskytují podporu pro řešení Detection and Response. Tato konfigurace se používá pro komplexní ochranu počítače před různými hrozbami, síťovými útoky a podvody.

Endpoint Detection and Response Agent. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

Light Agent na ochranu virtuálních prostředí. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Chránit infrastrukturu VDI** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

Součásti aplikace Kaspersky Endpoint Security

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



Výběr součástí aplikace k instalaci

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

- Ochrana před útoky BadUSB
- Součásti šifrování dat
- Součásti Detection and Response

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

Pokud potřebujete nainstalovat součásti Detection and Response, aplikace Kaspersky Endpoint Security podporuje následující konfigurace:

- Pouze Endpoint Detection and Response Optimum
- Pouze Endpoint Detection and Response Expert
- Pouze Endpoint Detection and Response (KATA)
- Pouze Network Detection and Response (KATA)
- Pouze Sandbox
- Endpoint Detection and Response Optimum a Sandbox
- Endpoint Detection and Response Expert a Sandbox
- Endpoint Detection and Response (KATA) a Sandbox
- Network Detection and Response (KATA) a Endpoint Detection and Response (KATA)
- Network Detection and Response (KATA) a Managed Detection and Response

Kaspersky Endpoint Security před instalací aplikace ověřuje výběr součástí. Pokud není podporována vybraná konfigurace součásti Detection and Response, aplikaci Kaspersky Endpoint Security nelze nainstalovat.

Výběr složky pro instalaci aplikace

Můžete změnit cestu instalace aplikace Kaspersky Endpoint Security v klientském počítači. Ve výchozím nastavení je aplikace nainstalována do složky `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.0`.

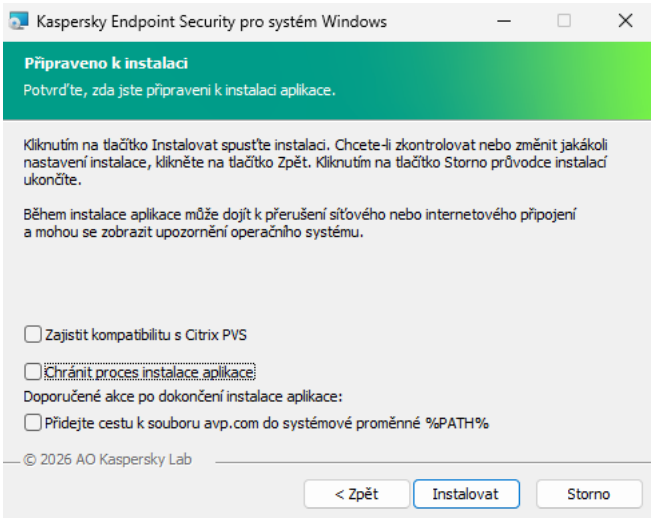
Konfigurace důvěryhodné zóny

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware.

Důvěryhodnou zónu můžete nakonfigurovat také později ve vlastnostech zásad: výjimky z kontroly a důvěryhodné aplikace.

Rozšířené nastavení



Rozšířené nastavení instalace aplikace

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 Windows Remote Desktop), doporučujeme ochranu instalace vypnout.

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

Přidejte cestu k souboru avp.com do systémové proměnné %PATH%. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku.

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 konzoly vyberte v bloku **Správa aplikací** položku **Balíčky**.
3. V horní části konzole klikněte na ovládacím panelu na tlačítko **Vytvořit balíček**.
   Spustí se *Průvodce vytvořením balíčku a programu*.
4. V Průvodci vytvořením balíčku a programu:
   a. V části **Balíček**:
      - V poli **Název** zadejte název instalačního balíčku.
      - V poli **Zdrojová složka** zadejte cestu ke složce obsahující distribuční balíček aplikace Kaspersky Endpoint Security.
   b. V části **Typ aplikace** vyberte možnost **Standardní program**.
   c. V části **Standardní program**:
      - V poli **Název** zadejte jedinečný název instalačního balíčku (například název aplikace včetně verze).
      - V poli **Příkazový řádek** určete možnosti instalace aplikace Kaspersky Endpoint Security z příkazového řádku.
      - Klikněte na tlačítko **Procházet** a určete cestu ke spustitelnému souboru aplikace.
      - Ujistěte se, že u seznamu **Režim spuštění** je vybrána položka **Spustit s právy správce**.
   d. V části **Požadavky**:

- Zaškrtněte políčko **Nejprve spusťte jiný program**, pokud chcete, aby byla před instalací aplikace Kaspersky Endpoint Security spuštěna jiná aplikace.

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

- Pokud si přejete, aby byla aplikace nainstalována pouze do určených operačních systémů, vyberte v bloku **Požadavky na platformu** možnost **Tento program může běžet pouze na určených platformách**.

  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 **Další**.

Vytvořený instalační balíček se zobrazí v části **Balíčky** 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 **Obecné**:

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

   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 **Další**.

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.

Soubor setup.ini používejte pouze při instalaci aplikace v bezobslužném režimu.

Cestu nelze přidat do souboru install.cfg konfiguračního souboru v souboru setup.ini. Aplikace také přeskočí konfigurační soubor install.cfg, pokud je tento soubor umístěn pouze ve složce s distribuční sadou aplikace Kaspersky Endpoint Security. Pokud chcete používat nastavení z konfiguračního souboru install.cfg, musíte zadat cestu k souboru v následujícím příkazu při instalaci aplikace: `CONFIGPATH=<path to the configuration file>`.

STAŽENÍ SOUBORU .INI

Soubor setup.ini se skládá z následujících částí:

- `[Setup]` – obecná nastavení instalace aplikace.
- `[Components]` – výběr součástí aplikace, které se mají instalovat ve standardním režimu. 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.
- `[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`, `enabled` a `true`. Místo hodnoty `0` lze použít hodnoty `no`, `off`, `disable`, `disabled` a `false`.

Část	Parametr	Popis
[Setup]	InstallDir	Cesta k instalační složce aplikace.
	ActivationCode	Aktivační kód aplikace Kaspersky Endpoint Security.
	Eula	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	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.
	CLEANERSIGNCHECK	Ověřování digitálních podpisů zjištěných souborů softwaru ze seznamu incompatible.txt. Chcete-li software odebrat, Kaspersky Endpoint Security spustí instalační soubor softwaru. Pokud instalační soubor nemá digitální podpis, aplikace Kaspersky Endpoint Security považuje soubor za nedůvěryhodný a zastaví odstraňování softwaru, aby se zabránilo spuštění potenciálně škodlivého kódu. Pokud aplikace nemůže ověřit digitální podpis zjištěného souboru softwaru, instalace aplikace Kaspersky Endpoint Security se zastaví s chybou. Výchozí hodnota se liší v závislosti na způsobu instalace softwaru: • 0 znamená, že ověřování digitálního podpisu je zakázáno (výchozí hodnota, pokud je aplikace nasazována prostřednictvím Kaspersky Security Center). • 1 znamená, že je povoleno ověřování digitálního podpisu (výchozí hodnota, pokud se aplikace instaluje lokálně).
	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. • EXPORT – export nastavení aplikace.

Například `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.

`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 Windows Remote Desktop), doporučujeme ochranu instalace vypnout.

`PROTECTOSSERVICES`

Ochrana funkce služeb operačního systému. Ochrana služeb operačního systému brání aplikacím třetích stran v narušení provozu služeb operačního systému. Mezi takové služby patří například služba automatického spouštění aplikace.

- `1` znamená, že je ochrana služeb operačního systému povolena (výchozí hodnota).
- `0` znamená, že je ochrana služeb operačního systému zakázána.

`EnableAzureSupport`

Povolení nebo zakázání režimu kompatibility Azure WVD. Dostupné hodnoty:

- `1` – Režim kompatibility Azure WVD je povolen.
- `0` – Režim kompatibility Azure WVD je zakázán (výchozí hodnota).

Tato funkce zajišťuje správné zobrazení stavu virtuálního počítače Azure v konzole Kaspersky Anti Targeted Attack Platform. Pro sledování výkonu počítače odesílá Kaspersky Endpoint Security telemetrii na servery KATA. Telemetrie zahrnuje ID počítače (Sensor ID). Režim kompatibility Azure WVD umožňuje těmto virtuálním počítačům přiřadit trvalé jedinečné Sensor ID. Pokud je režim kompatibility vypnutý, Sensor ID se může po restartování počítače změnit kvůli tomu, jak fungují virtuální počítače Azure. To může způsobit, že se na konzole objeví duplikáty virtuálních počítačů.

`Reboot`

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.

`UPGRADEMODE`

Režim upgradu aplikace:

- `Seamless` znamená upgrade aplikace s restartem počítače (výchozí hodnota).
- `Force` znamená upgrade aplikace bez restartování.

Aplikaci můžete upgradovat bez restartu od verze 11.10.0. Chcete-li upgradovat starší verzi aplikace, musíte restartovat počítač. Od verze 11.11.0 můžete bez restartování rovněž instalovat bezpečnostní opravy.

Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Režim upgradu aplikace bude tedy určen v nastavení aplikace. Tento parametr můžete změnit v nastavení aplikace nebo v zásadách.

	Při upgradu již nainstalované aplikace je priorita parametru uvedeného v souboru setup.ini vyšší než priorita parametru uvedeného v nastavení aplikace nebo v příkazovém řádku. Například pokud je v souboru setup.ini zadán režim upgradu `Force` a v nastavení aplikace je zadán režim `Seamless`, upgrade se nainstaluje bez restartu (`Force`). Jestliže používáte soubor setup.ini, kde není zadán parametr `UPGRADEMODE`, instalační program použije výchozí hodnotu (`Seamless`) a nainstaluje upgrade s restartováním počítače.
`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.14.0\Traces`. Dostupné hodnoty: • `1` – trasování aplikací je povoleno. • `0` – trasování aplikací je zakázáno (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. Ujistěte se, že je port volný.
`RESTAPI_Certificate`	Certifikát pro identifikaci požadavků (např. `RESTAPI_Certificate=C:\cert.pem`). Zabezpečená interakce aplikace Kaspersky Endpoint Security s klientem REST vyžaduje konfiguraci identifikace požadavku. K tomu musíte nainstalovat certifikát a následně podepsat payload každého požadavku.
`StandaloneMode`	Instalace aplikace v režimu Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* je aplikace, která se instaluje na jednotlivé pracovní stanice a servery v IT infrastruktuře organizace za účelem podpory řešení Kaspersky Managed Detection and Response a Kaspersky Anti Targeted Attack Platform. EDR Agent je kompatibilní s aplikacemi EPP třetích stran. To vám umožní používat spolu s řešením Detection and Response od společnosti Kaspersky nástroje zabezpečení infrastruktury třetích stran. Chcete-li nainstalovat EDR Agent, v části `[Components]` vyberte součásti `StandaloneKATA`, `StandaloneNDR` nebo `StandaloneMDR`. EDR Agent nepodporuje jiné součásti aplikace. Dostupné hodnoty: • `1` pro instalaci aplikace v režimu EDR Agent. • `0` pro instalaci aplikace ve standardním režimu (výchozí).
`KSVLAMode`	Instalace aplikace v režimu Light Agent. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. Dostupné hodnoty:

- `1` pro instalaci aplikace v režimu Light Agent.
- `0` pro instalaci aplikace ve standardním režimu (výchozí).

	`InstallOnVDI`	Povolení režimu ochrany VDI při instalaci aplikace v režimu Light Agent (`KSVLAMode=1`). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů. Dostupné hodnoty: • `1` povolí režim ochrany VDI. • `0` zakáže režim ochrany VDI (výchozí).
	`KESExclusions`	Přidání předdefinovaných výjimek z kontroly a důvěryhodných aplikací při instalaci aplikace na server. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. Například předdefinované výjimky z kontroly pro servery SQL zahrnují databázové soubory MDF a LDF. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Dostupné hodnoty: • `1` povolí předdefinované výjimky z kontroly a důvěryhodné aplikace. • `0` zakáže předdefinované výjimky z kontroly a důvěryhodné aplikace.
	`LAExclusions`	Přidání předdefinovaných výjimek z kontroly a důvěryhodných aplikací při instalaci aplikace na virtuální počítač (režim Light Agent). Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware. Dostupné hodnoty: • `1` povolí předdefinované výjimky z kontroly a důvěryhodné aplikace. • `0` zakáže předdefinované výjimky z kontroly a důvěryhodné aplikace.
	`EnableUniqueSensorID`	Vytvoření jedinečného identifikátoru počítače (Sensor ID) během instalace nebo aktualizace aplikace. Sensor ID se v řešení Kaspersky Anti Targeted Attack Platform používá k identifikaci počítačů, které odesílají telemetrii na server. Při vytváření Sensor ID aplikace používá algoritmus, který bere v úvahu konfiguraci počítače, jako je například sériové číslo základní desky. V některých případech, například při používání aplikace ve virtuálním prostředí, může dojít k duplikaci Sensor ID. Kaspersky Anti Targeted Attack Platform tak nemůže identifikovat počítač, ze kterého je telemetrie odesílána. Chcete-li vytvořit jedinečné Sensor ID, musíte nastavit parametr `EnableUniqueSensorID=1`. Aplikace tak k vytvoření identifikátoru Sensor ID použije jiný algoritmus, který bere v úvahu jiná data o počítači. Tím je zajištěna jedinečnost Sensor ID. Ve výchozím nastavení není parametr nastaven. Aplikace zdědí Sensor ID v následujících případech: • aktualizace verze aplikace; • migrace konfigurace [KES+KEA] na konfiguraci [KES+integrovaný agent]. V rámci opravy aplikace se instalační program pokusí zdědit Sensor ID. Pokud Sensor ID nelze obnovit, aplikace vytvoří nový Sensor ID.
	`CitrixCompatibility`	Povolení podpory služeb Citrix Provisioning Services za účelem instalace aplikace Kaspersky Endpoint Security do virtuálního počítače.
`[Components]`	`ALL`	Instalace všech součástí. Pokud je zadána hodnota parametru `1`, nainstalují se všechny součásti bez ohledu na nastavení instalace pro jednotlivé součásti. Vzhledem ke způsobu, jakým jsou podporována řešení Detection and Response, jsou do počítače nainstalovány součásti Endpoint Detection and Response Optimum a Kaspersky Sandbox. Součást Endpoint Detection and Response Expert není kompatibilní s touto konfigurací.
	`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.
`Firewall`	Brána firewall.
`NetworkThreatProtection`	Ochrana před síťovými hrozbami.
`WebControl`	Kontrola webu
`DeviceControl`	Kontrola zařízení.
`ApplicationControl`	Kontrola aplikací.
`AdaptiveAnomaliesControl`	Adaptivní kontrola anomálií.
`CloudDiscovery`	Cloud Discovery.
`LogInspector`	Kontrola protokolu
`AntiCryptor`	Anti-Cryptor
`FileThreatProtection`	Ochrana před souborovými hrozbami
`SystemIntegrityMonitor`	Monitorování integrity systému.
`FileEncryption`	Knihovny šifrování na úrovni souborů.
`DiskEncryption`	Knihovny úplného šifrování disku.
`MSBitLocker`	Knihovny pro správu šifrování nástrojem BitLocker.
`BadUSBAttackPrevention`	Ochrana před útoky BadUSB.
`EDR`	Endpoint Detection and Response Optimum (EDR Optimum). Součást není kompatibilní se součástmi EDR Expert (`EDRCloud`) a EDR (KATA) (`EDRKATA`).
`EDRCloud`	Endpoint Detection and Response Expert (EDR Expert). Součást není kompatibilní se součástmi EDR Optimum (`EDR`) a EDR (KATA) (`EDRKATA`).
`AntiAPT`	Endpoint Detection and Response (KATA). Součást není kompatibilní se součástmi EDR Expert (`EDRCloud`) a EDR Optimum (`EDR`).
`SB`	Kaspersky Sandbox nebo KATA Sandbox. *Kaspersky Sandbox* je samostatné řešení Detection and Response od společnosti Kaspersky. *KATA Sandbox* je součástí řešení Kaspersky Anti Targeted Attack Platform.
`MDR`	Managed Detection and Response.
`NDR`	Network Detection and Response (KATA). Součást není kompatibilní se součástmi EDR Expert (`EDRCloud`) a EDR Optimum (`EDR`).

	`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.
	`KUMAIntegration`	Integrace s KUMA.
	`StandaloneKATA`	Instalace aplikace v režimu Endpoint Detection and Response Agent (EDR Agent) pro integraci s řešením Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Instalace aplikace v režimu Endpoint Detection and Response Agent (EDR Agent) pro integraci s řešením Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Instalace aplikace v režimu Endpoint Detection and Response Agent (EDR Agent) pro integraci s řešením Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Instalace aplikace v režimu Endpoint Detection and Response Agent (EDR Agent) pro integraci s KUMA.
`[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.

  > Tato metoda není dostupná, pokud byla aplikace nainstalována prostřednictvím aplikace Kaspersky Security Center. Výběr součástí aplikace v Ovládacích panelech můžete změnit až po místní instalaci aplikace.

- Vzdáleně prostřednictvím aplikace Kaspersky Security Center.

  Úloha *Změna součástí 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.
- Pokud je aplikace nainstalované v režimu Light Agent v infrastruktuře VDI, změna nastavených součástí není podporována.

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

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Výběr součástí k instalaci**.

Krok 2. Nastavení úlohy pro změnu součástí aplikace

Vyberte konfiguraci aplikace:

- **Standardní režim pro ochranu hostitelů**. Výchozí konfigurace. Tato konfigurace vám umožňuje používat všechny součásti aplikace, včetně součástí, které poskytují podporu pro řešení Detection and Response. Tato konfigurace se používá pro komplexní ochranu počítače před různými hrozbami, síťovými útoky a podvody.
- **Endpoint Detection and Response Agent na ochranu před pokročilými hrozbami a cílenými útoky**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

  Při změně konfigurace aplikace, aby agent EDR Agent fungoval s MDR, se ujistěte, že jsou povoleny součásti odpovědné za příjem telemetrie.

- **Light Agent na ochranu virtuálních prostředí**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Chránit infrastrukturu VDI** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

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

Krok 3. Rozšířené nastavení

Nakonfigurujte rozšířené nastavení pro úlohu (viz tabulka níže).

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. Konfigurace plánu spuštění úlohy

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

Krok 6. Definování názvu úlohy

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

Krok 7. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

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

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Change application components**.
3. V poli **Task name** zadejte krátký popis, například *Přidání součásti Kontrola aplikací.*
4. V bloku **Devices to which the task will be assigned** 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 **Open task details when creation is complete** a dokončete průvodce.

Ve vlastnostech úlohy vyberte část **Application settings**. Dále vyberte konfiguraci aplikace:

- **Standard mode to protect workstations and servers**. Výchozí konfigurace. Tato konfigurace vám umožňuje používat všechny součásti aplikace, včetně součástí, které poskytují podporu pro řešení Detection and Response. Tato konfigurace se používá pro komplexní ochranu počítače před různými hrozbami, síťovými útoky a podvody.
- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

  Při změně konfigurace aplikace, aby agent EDR Agent fungoval s MDR, se ujistěte, že jsou povoleny součásti odpovědné za příjem telemetrie.

- **Light Agent to protect virtual environments**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Protect VDI infrastructure** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

Vyberte součásti aplikace, které budou k dispozici v počítači uživatele. Nakonfigurujte rozšířené nastavení pro úlohu (viz tabulka níže).

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.

Při instalaci, aktualizaci nebo odinstalaci aplikace Kaspersky Endpoint Security může dojít k chybám. Další informace o řešení těchto chyb naleznete ve znalostní bázi technické podpory.

Rozšířené nastavení úlohy

Parametr	Popis

Nastavení úlohy	**Vyhledávat nekompatibilní aplikace třetích stran**. Ve výchozím nastavení Kaspersky Endpoint Security zkontroluje kompatibilitu nainstalovaných aplikací. Seznam softwaru, který může způsobovat problémy s kompatibilitou, je k dispozici v souboru incompatible.txt. Tento soubor je součástí distribučního balíčku. Pokud je povolena kontrola nainstalovaného softwaru a je zjištěna aplikace ze seznamu, Kaspersky Endpoint Security úlohu zastaví. Kontrolu nainstalovaného softwaru můžete zakázat, pokud dokumentace dodavatele softwaru třetí strany uvádí kompatibilitu s EPP (Endpoint Protection Platform). **Odebrat nekompatibilní aplikace třetích stran**. Automatické odebrání aplikací uvedených v souboru incompatible.txt před změnou kombinace součástí. Je-li tato funkce povolena, aplikace Kaspersky Endpoint Security se pokusí odebrat aplikace, které mohou způsobovat problémy s kompatibilitou, aby mohla úloha pokračovat. **Použít režim kompatibility Azure WVD**. Tato funkce zajišťuje správné zobrazení stavu virtuálního počítače Azure v konzole Kaspersky Anti Targeted Attack Platform. Pro sledování výkonu počítače odesílá Kaspersky Endpoint Security telemetrii na servery KATA. Telemetrie zahrnuje ID počítače (Sensor ID). Režim kompatibility Azure WVD umožňuje těmto virtuálním počítačům přiřadit trvalé jedinečné Sensor ID. Pokud je režim kompatibility vypnutý, Sensor ID se může po restartování počítače změnit kvůli tomu, jak fungují virtuální počítače Azure. To může způsobit, že se na konzole objeví duplikáty virtuálních počítačů.
Výjimky	Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware. Důvěryhodnou zónu můžete nakonfigurovat také později ve vlastnostech zásad: výjimky z kontroly a důvěryhodné aplikace.
Samostatný režim / Kombinovaný režim	Pro pracovní stanici a servery můžete vytvořit samostatné kombinace součástí – **Samostatný režim**. Před nasazením instalačního balíčku instalační program zjistí typ operačního systému a nainstaluje pouze ty součásti aplikace, které jste vybrali pro daný typ operačního systému. Stejný instalační balíček tak můžete použít pro pracovní stanice i servery. **Kombinovaný režim** nabízí běžný seznam součástí pro pracovní stanice a servery. Dostupnost jednotlivých součástí závisí na typu operačního systému. V tomto režimu doporučujeme vytvořit samostatný instalační balíček pro pracovní stanice a samostatný instalační balíček pro servery. Běžný seznam součástí v instalačním balíčku můžete nakonfigurovat pouze ve standardním režimu.
Použít pro úpravy sady součástí aplikace heslo	Správci obvykle povolují ochranu heslem, aby omezili přístup k aplikaci Kaspersky Endpoint Security. To znamená, že chcete-li upravit výběr součástí aplikace, musíte zadat přihlašovací údaje uživatele, který má toto oprávnění **Odebrat/změnit/obnovit aplikaci**. Můžete například použít účet KLAdmin.
Použít k odinstalaci aplikace Kaspersky Endpoint Agent a Kaspersky Security for Windows Server heslo	Správci obvykle povolují ochranu heslem v nastavení těchto úloh, aby omezili přístup k aplikaci Kaspersky Endpoint Agent (KEA) a Kaspersky Security for Windows Server (KSWS). To znamená, že pokud migrujete z konfigurace [KES+KEA] na [KES+integrovaný agent] nebo pokud migrujete z KSWS na KES, musíte pro odebrání těchto aplikací zadat heslo.

Upgradování předchozí verze aplikace

Při aktualizaci předchozí verze aplikace na novější verzi zvažte následující:

- Lokalizace nové verze aplikace Kaspersky Endpoint Security musí odpovídat lokalizaci nainstalované verze aplikace. Pokud se lokalizace aplikací neshodují, upgrade aplikace bude dokončen s chybou.
- Před zahájením aktualizace doporučujeme ukončit všechny aktivní aplikace.
- 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 12.1 pro systém Windows (sestavení 12.1.0.506)
- Kaspersky Endpoint Security 12.2 pro systém Windows (sestavení 12.2.0.462)
- Kaspersky Endpoint Security 12.3 pro systém Windows (sestavení 12.3.0.493)
- Kaspersky Endpoint Security 12.4 pro systém Windows (sestavení 12.4.0.467)
- Kaspersky Endpoint Security 12.5 pro systém Windows (sestavení 12.5.0.539)
- Kaspersky Endpoint Security 12.6 pro systém Windows (sestavení 12.6.0.438)
- Kaspersky Endpoint Security 12.7 pro systém Windows (sestavení 12.7.0.533)

- Kaspersky Endpoint Security 12.8 pro systém Windows (sestavení 12.8.0.505)
- Kaspersky Endpoint Security 12.9 pro systém Windows (sestavení 12.9.0.384)
- Kaspersky Endpoint Security 12.10 pro systém Windows (sestavení 12.10.0.466)
- Kaspersky Endpoint Security 12.11 pro systém Windows (sestavení 12.11.0.637)
- Kaspersky Endpoint Security 12.12 pro systém Windows (sestavení 12.12.0.522)

Při instalaci, aktualizaci nebo odinstalaci aplikace Kaspersky Endpoint Security může dojít k chybám. Další informace o řešení těchto chyb naleznete ve znalostní bázi technické podpory.

Způsoby upgradu aplikace

Aplikaci Kaspersky Endpoint Security lze v počítači aktualizovat několika způsoby:

- pomocí aktualizační služby Kaspersky (Seamless Update – SMU),
- místně pomocí průvodce instalací,
- místně z příkazového řádku,
- vzdáleně prostřednictvím aplikace Kaspersky Security Center,
- vzdáleně prostřednictvím editoru správy zásad skupiny v systému Microsoft Windows (další podrobnosti najdete na webu 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.

Upgrade aplikace bez restartování

Upgrade aplikace bez restartování zajišťuje nepřerušený provoz serveru při aktualizaci verze aplikace.

Upgrade aplikace bez restartu má následující omezení:

- Aplikaci můžete upgradovat bez restartu od verze 11.10.0. Chcete-li upgradovat starší verzi aplikace, musíte restartovat počítač.
- Aplikaci můžete upgradovat bez restartu od verze 11.11.0. Pro instalaci bezpečnostních oprav pro starší verze aplikace může být nutný restart počítače.
- Upgrade aplikace bez restartu není dostupná na počítačích se zapnutým šifrováním dat (šifrování Kaspersky (FDE), BitLocker, šifrování na úrovni souborů (FLE)). Chcete-li upgradovat aplikaci v počítačích se zapnutým šifrováním dat, je třeba počítač restartovat.
- Aplikaci nelze upgradovat na virtuálním počítači bez restartování. Chcete-li upgradovat aplikaci na virtuálním počítači, musíte virtuální počítač restartovat.

Po upgradu aplikace, instalaci opravy, změně kombinace součástí aplikace nebo obnovení se aplikace Kaspersky Endpoint Security restartuje, aby začala používat novou verzi. Restartování aplikace Kaspersky Endpoint Security může trvat až jednu minutu. Během této doby je úroveň ochrany počítače snížena. Po restartování aplikace se obnoví úroveň ochrany počítače.

Jak vybrat režim upgradu aplikace v konzole pro správu (MMC)

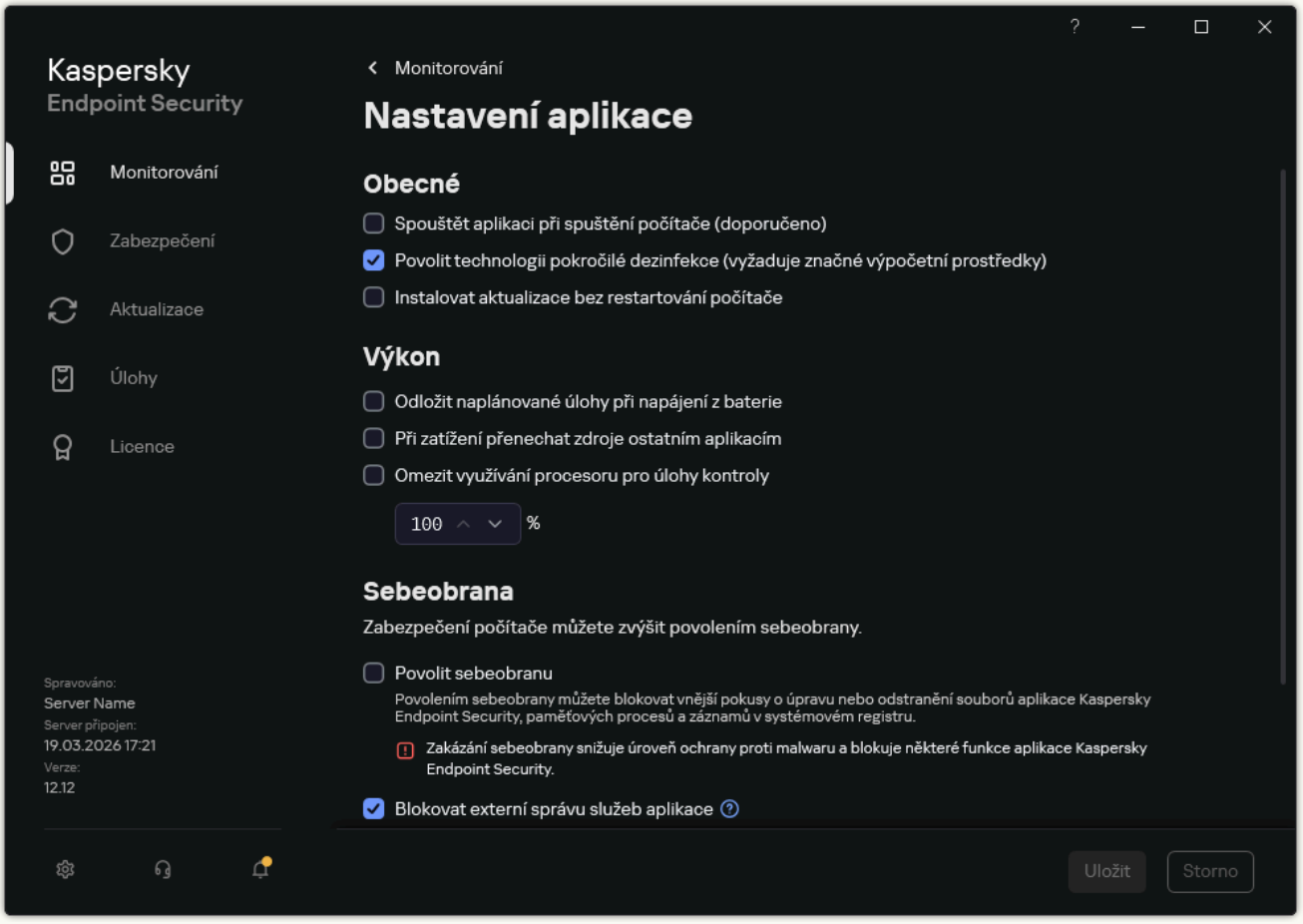
1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **User Interaction**.
5. V bloku **Application update settings** zaškrtnutím políčka **Install application updates without restart** nebo zrušením jeho zaškrtnutí nakonfigurujete režim aktualizace aplikace.
6. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V bloku **Rozšířené nastavení** zaškrtnutím políčka **Nainstalovat aktualizace aplikace bez restartování počítače** nebo zrušením jeho zaškrtnutí nakonfigurujete režim aktualizace aplikace.
5. Uložte změny.

Jak vybrat režim upgradu aplikace v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. V bloku **Obecné** zaškrtnutím políčka **Instalovat aktualizace bez restartování počítače** nebo zrušením jeho zaškrtnutí nakonfigurujete režim aktualizace aplikace.

4. Uložte změny.

Po dokončení upgradu aplikace bez restartování bude do počítače nainstalována nová verze aplikace Kaspersky Endpoint Security. Předchozí verze aplikace je automaticky odstraněna.

Upgrade aplikace nelze spustit před úplným dokončením předchozího upgradu.

Stav upgradu aplikace Kaspersky Endpoint Security můžete zkontrolovat pomocí zprávy o verzi aplikace Kaspersky v konzole aplikace Kaspersky Security Center.

Aktualizace SMU aplikace

Chcete-li aktualizovat aplikaci pomocí aktualizační služby Kaspersky (Seamless Update; SMU), nemusíte na rozdíl od jiných způsobů aktualizace spouštět instalační program. Kaspersky Endpoint Security získává novou verzi aplikace spolu s antivirovými databázemi z téhož zdroje.

Aktualizace SMU umožňuje aktualizaci aplikace na všech počítačích vaší organizace na nejnovější verzi. Před použitím aktualizace SMU doporučujeme otestovat novou verzi aplikace na několika počítačích. Chcete-li tak učinit, musíte aplikaci na těchto počítačích aktualizovat ručně (například lokálně pomocí průvodce instalací). Při provádění aktualizace SMU nemůžete vybrat jednotlivé počítače.

Plán aktualizace aplikace určují pracovníci společnosti Kaspersky. Aby bylo zajištěno hladké fungování nové verze aplikace, Kaspersky zpřístupňuje aktualizace postupně. To znamená, že aktualizaci SMU můžete získat až o dva měsíce později, než je vydání nové verze.

Aktualizaci SMU aplikace můžete spravovat pomocí úlohy *Aktualizace databází a modulů aplikace*. Chcete-li mít novou verzi aplikace v ráci stejného balíčku jako antivirové databáze, musíte povolit aktualizaci *modulů aplikace* v nastavení úlohy *Aktualizace databází a modulů aplikace*. Rovněž v nastavení úlohy *Aktualizace databází a modulů aplikace* můžete umožnit aktualizaci aplikace bez restartu.

Kroky aktualizace aplikace SMU

1. **Po vydání nové verze aplikace společnost Kaspersky distribuuje aktualizaci.**

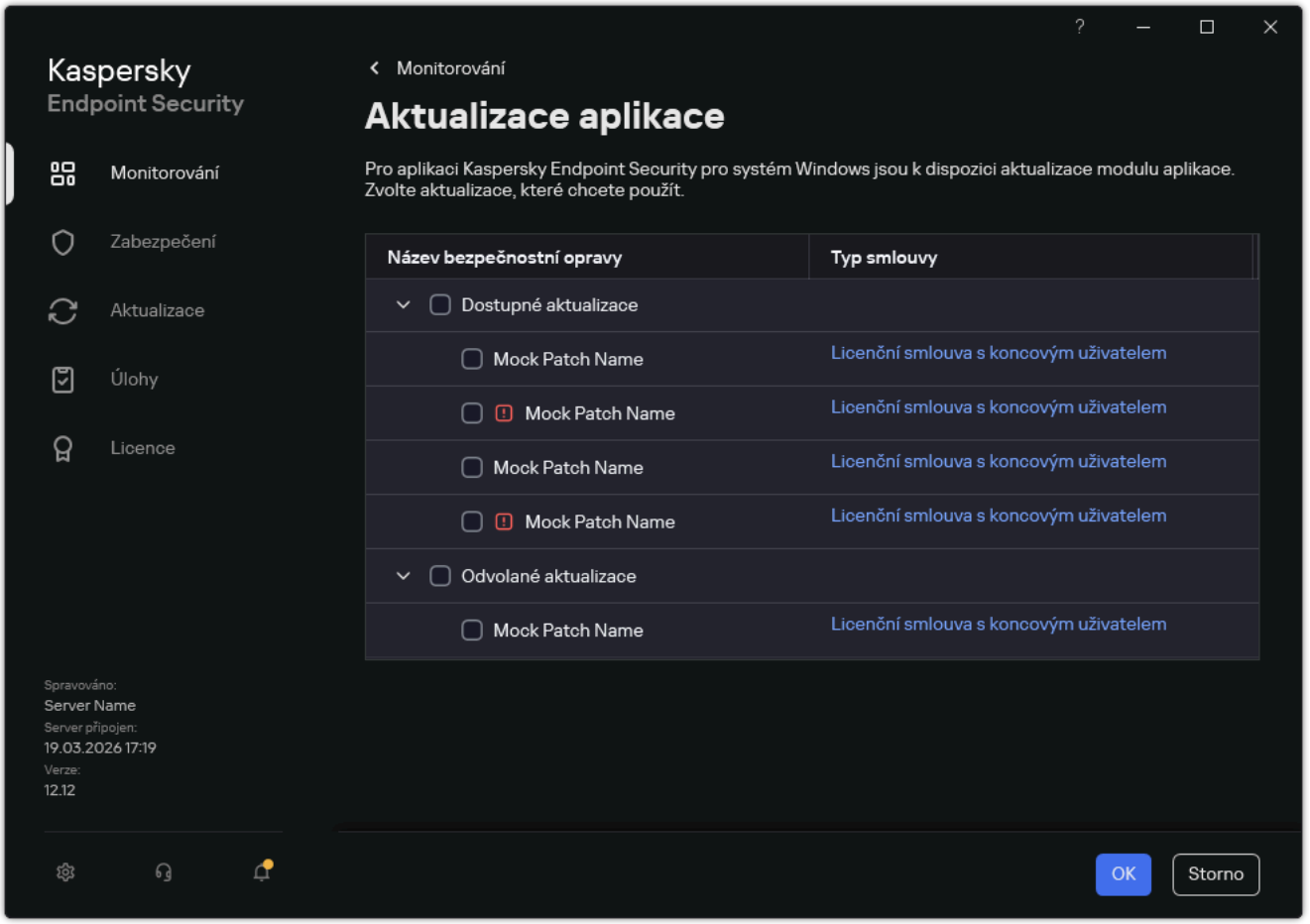
2. **Uživatel schvaluje aktualizaci aplikace.**

   Pokud je počítač připojen k aplikaci Kaspersky Security Center, aktualizace je k dispozici v aplikaci Kaspersky Security Center, v části **Update of Kaspersky databases and application modules**. Další informace o schvalování aktualizací najdete v nápovědě k aplikaci Kaspersky Security Center.

   Pokud počítač není připojen k aplikaci Kaspersky Security Center, aktualizace je k dispozici v oznamovací části rozhraní aplikace: . Chcete-li aktualizaci schválit, vyberte verzi aplikace a přijměte podmínky smluv (viz obrázek níže).

3. **Kaspersky Endpoint Security provádí úlohu *Aktualizace databází a modulů aplikace* v souladu s nakonfigurovaným plánem.**

Aplikace Kaspersky Endpoint Security tak aktualizuje aplikaci v bezobslužném režimu.



Dostupné aktualizace aplikací

Odebrání aplikace

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

Při instalaci, aktualizaci nebo odinstalaci aplikace Kaspersky Endpoint Security může dojít k chybám. Další informace o řešení těchto chyb naleznete ve znalostní bázi technické podpory.

Vzdálené odebrání aplikace prostřednictvím aplikace Kaspersky Security Center

Aplikaci můžete vzdáleně odinstalovat pomocí úlohy *Uninstall application remotely*. 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. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
   Otevře se seznam úloh.
3. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte položky **Kaspersky Security Center Administration Server** → **Advanced** → **Uninstall application remotely**.

Krok 2. Výběr aplikace, která má být odebrána

Vyberte možnost **Uninstall application supported by Kaspersky Security Center**.

Krok 3. Nastavení úlohy pro odinstalování aplikace

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)**.

Krok 4. Odinstalace nastavení nástroje

Nakonfigurujte následující další nastavení aplikace:

- **Force download of the uninstallation utility**. Vyberte způsob doručení nástroje:
  - **Using 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.
  - **Using operating system resources through Administration Server**. 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.
  - **Using operating system resources through distribution points**. 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.
- **Verify operating system type before downloading**. 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 **Use uninstallation password**.
2. Klikněte na tlačítko **Edit**.
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 14.0*.

Krok 10. Vytvoření úloh po dokončení

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. 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 konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Security Center**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Uninstall application remotely**.
3. Do pole **Task name** zadejte krátký popis, například *Odinstalace aplikace Kaspersky Endpoint Security z počítačů technické podpory.*
4. V bloku **Devices to which the task will be assigned** 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 typ **Uninstall managed application**.
2. Vyberte možnost **Kaspersky Endpoint Security for Windows**.
3. **Force download of the uninstallation utility**. Vyberte způsob doručení nástroje:
   - **Using 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.
   - **Using operating system resources through Administration Server**. 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.
   - **Using operating system resources through distribution points**. 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 **Maximum number of concurrent downloads** 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 **Maximum number of uninstallation attempts** 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 **Verify operating system type before downloading**. 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 **Finish** 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 *Uninstall application remotely* heslo k účtu KLAdmin. Bez hesla nebude úloha provedena.

Použití hesla k účtu KLAdmin v úloze Uninstall application remotely:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na úlohu **Uninstall application remotely** aplikace Kaspersky Security Center.
   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Application settings**.
4. Zaškrtněte políčko **Use uninstallation password**.
5. Zadejte heslo k účtu KLAdmin.
6. Uložte změny.

Odinstalaci dokončíte restartováním počítače. K tomu součást Network Agent zobrazí vyskakovací okno.

Vzdálené odebrání aplikace pomocí služby Active Directory

Aplikaci můžete vzdáleně odinstalovat pomocí zásad skupiny systému Microsoft Windows. Chcete-li aplikaci odinstalovat, musíte otevřít konzolu pro správu zásad skupiny (gpmc.msc) a pomocí editoru zásad skupiny vytvořit úlohu odebrání aplikace (další podrobnosti naleznete na webu technické podpory společnosti Microsoft).

Pokud je operace odinstalování aplikace chráněna heslem, musíte postupovat takto:

1. Vytvořte soubor BAT s následujícím obsahem:

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

   `<GUID>` je jedinečný identifikátor aplikace. GUID aplikace můžete zjistit ve znalostní bázi technické podpory nebo pomocí následujícího příkazu:

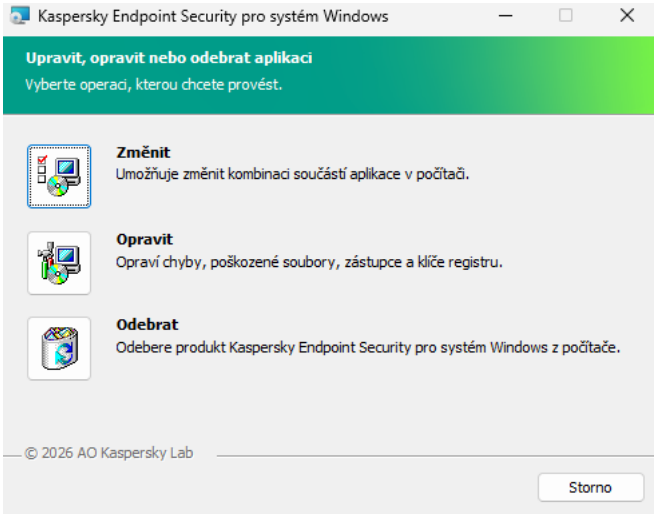
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber

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

2. V konzole pro správu zásad skupiny (gpmc.msc) vytvořte pro počítače novou zásadu systému Microsoft Windows.
3. Pomocí této nové zásady spusťte v počítačích vytvořený soubor BAT.

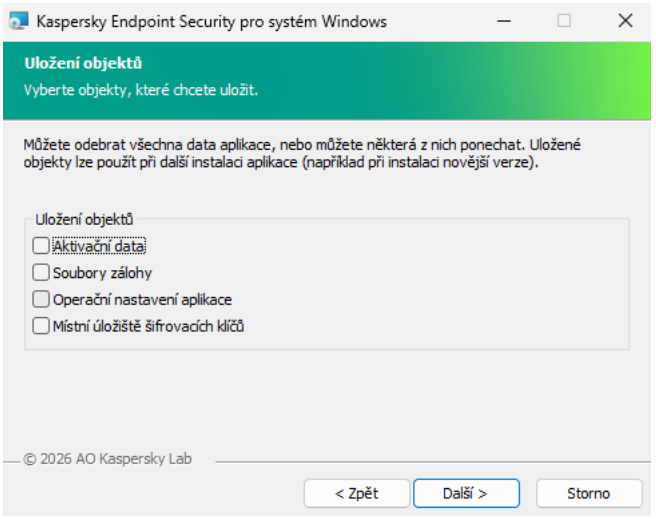
Místní odebrání aplikace

Aplikaci můžete odebrat místně pomocí průvodce instalací. 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.



Výběr operace odebrání aplikace

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 nezadáte žádné údaje, aplikace bude zcela odebrána (viz obrázek níže).



Uložení dat po odebrání

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.

Aplikace Kaspersky Endpoint Security ukládá data do složky `C:\ProgramData\Kaspersky Lab\KES.14.0\QB`.

Aplikaci můžete odstranit místně také pomocí příkazového řádku.

Poskytování licence na aplikaci

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

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\KES\Doc\<locale>\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.

Licence vás opravňuje k používání aplikace v souladu s podmínkami licenční smlouvy s koncovým uživatelem a k získání technické podpory. Seznam dostupných funkcí a možností využívání 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. Aplikaci nelze aktivovat v rámci zkušební licence poté, co byla aktivována s komerční licencí.

- *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 ID 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. Aplikaci nelze aktivovat v rámci předplatného pomocí souboru klíče. Poskytovatel služeb může poskytnout pouze aktivační kód. V rámci předplatného není možné přidat rezervní 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 použitím 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 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

Key file 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.

- Získejte soubor klíče z jiného serveru pro správu.

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

Porovnání fungování aplikací v závislosti na typu licence pro pracovní stanice

Soubor funkcí aplikace Kaspersky Endpoint Security dostupných na pracovních stanicích závisí na typu licence (viz tabulka níže).

Viz také srovnání funkcí aplikací pro servery

Porovnání funkčnosti aplikace v závislosti na typu licence Kaspersky Next najdete v nápovědě k aplikaci Kaspersky Next.

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Rozšířená ochrana před hrozbami								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detekce chování	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
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 protokolu	–	–	–	–	–	–	–	–
Kontrola aplikací	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola zařízení	✓	✓	✓	✓	✓	✓	✓	✓
Kontrola webu	✓	✓	✓	✓	✓	✓	✓	✓
Adaptivní kontrola anomálií	–	✓	✓	✓	✓	✓	–	✓
Monitorování integrity systému	–	–	–	–	–	–	–	–
Šifrování dat								

Kaspersky Disk Encryption	–	✓	✓	✓	✓	✓	–	✓
BitLocker Drive Encryption	–	✓	✓	✓	✓	✓	–	✓
Šifrování na úrovni souborů	–	✓	✓	✓	✓	✓	–	✓
Šifrování vyměnitelných jednotek	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Licenci k řešení Kaspersky Sandbox je nutno zakoupit samostatně)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrace s KUMA *(licenci pro integraci KUMA je nutné zakoupit samostatně)*	✓	✓	✓	✓	✓	✓	✓	✓
Režim Light Agent *(chcete-li aktivovat aplikaci, musíte na server SVM, ke které je součást Light Agent připojena, přidat licenční klíč)*	–	–	–	–	–	–	✓	✓

Porovnání fungování aplikací v závislosti na typu licence pro servery

Soubor funkcí aplikace Kaspersky Endpoint Security dostupných na serverech závisí na typu licence (viz tabulka níže).

Viz také srovnání funkcí aplikací pro pracovní stanice

Porovnání funkčnosti aplikace v závislosti na typu licence Kaspersky Next najdete v nápovědě k aplikaci Kaspersky Next.

Porovnání funkcí aplikace Kaspersky Endpoint Security

Funkce	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Rozšířená ochrana před hrozbami								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Detekce chování	✓	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor	✓	✓	✓	✓	✓	✓	✓	✓
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 protokolu	–	–	–	–	–	–	–	✓
Kontrola aplikací	–	✓	✓	✓	✓	✓	–	✓
Kontrola zařízení	–	✓	✓	✓	✓	✓	✓	✓
Kontrola webu	–	✓	✓	✓	✓	✓	✓	✓
Adaptivní kontrola anomálií	–	–	–	–	–	–	–	–
Monitorování integrity systému	–	–	–	–	–	–	–	✓
Šifrování dat								
Kaspersky Disk Encryption	–	–	–	–	–	–	–	–
BitLocker Drive Encryption	–	✓	✓	✓	✓	✓	–	✓
Šifrování na úrovni souborů	–	–	–	–	–	–	–	–
Šifrování vyměnitelných jednotek	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Licenci k řešení Kaspersky Sandbox je nutno zakoupit samostatně)*	✓	✓	✓	✓	✓	✓	✓	✓
Integrace s KUMA *(licenci pro integraci KUMA je nutné zakoupit samostatně)*	✓	✓	✓	✓	✓	✓	✓	✓
Režim Light Agent	–	–	–	–	–	–	✓	✓

(chcete-li aktivovat aplikaci, musíte na server SVM, ke které je součást Light Agent připojena, přidat licenční klíč)

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:

- Lokálně z rozhraní aplikace pomocí průvodce aktivací. Tímto způsobem můžete přidat aktivní klíč a rezervní klíč.
- Vzdáleně pomocí softwarové sady Kaspersky Security Center.
  - Pomocí úlohy *Přidání klíče*.

    Tento způsob umožňuje přidat klíč do konkrétního počítače nebo počítačů, které jsou součástí skupiny pro správu. Tímto způsobem můžete přidat aktivní klíč a rezervní klíč.
  - 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 nápovědě k aplikaci Kaspersky Security Center.

    > Nejprve je distribuován aktivační kód zakoupený v rámci předplatného.

  - Přidáním klíče do instalačního balíčku aplikace Kaspersky Endpoint Security.

    Tato metoda vám umožňuje přidat při nasazování aplikace Kaspersky Endpoint Security klíč do vlastností instalačního balíčku. Aplikace se po instalaci automaticky aktivuje.
- 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.

> Pokud se aplikace Kaspersky Endpoint Security používá v režimu Light Agent pro ochranu virtuálních prostředí, není nutné aplikaci aktivovat samostatně.

Aktivace aplikace

Jak aktivovat aplikaci v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Přidání klíče**.

Krok 2. Přidání klíče

Zadejte aktivační kód nebo vyberte soubor klíče.

Podrobnosti o přidání klíčů do úložiště aplikace Kaspersky Security Center najdete v nápovědě 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 **Run the task after the wizard finishes**. 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 konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Add key**.
3. V poli **Task name** zadejte krátký popis, například *Aktivace aplikace Kaspersky Endpoint Security pro systém Windows*.
4. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy. Přejděte k dalšímu kroku.

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. Přejděte k dalšímu kroku.

Klíče můžete přidat do webové konzoly (**Operations** → **Licensing**).

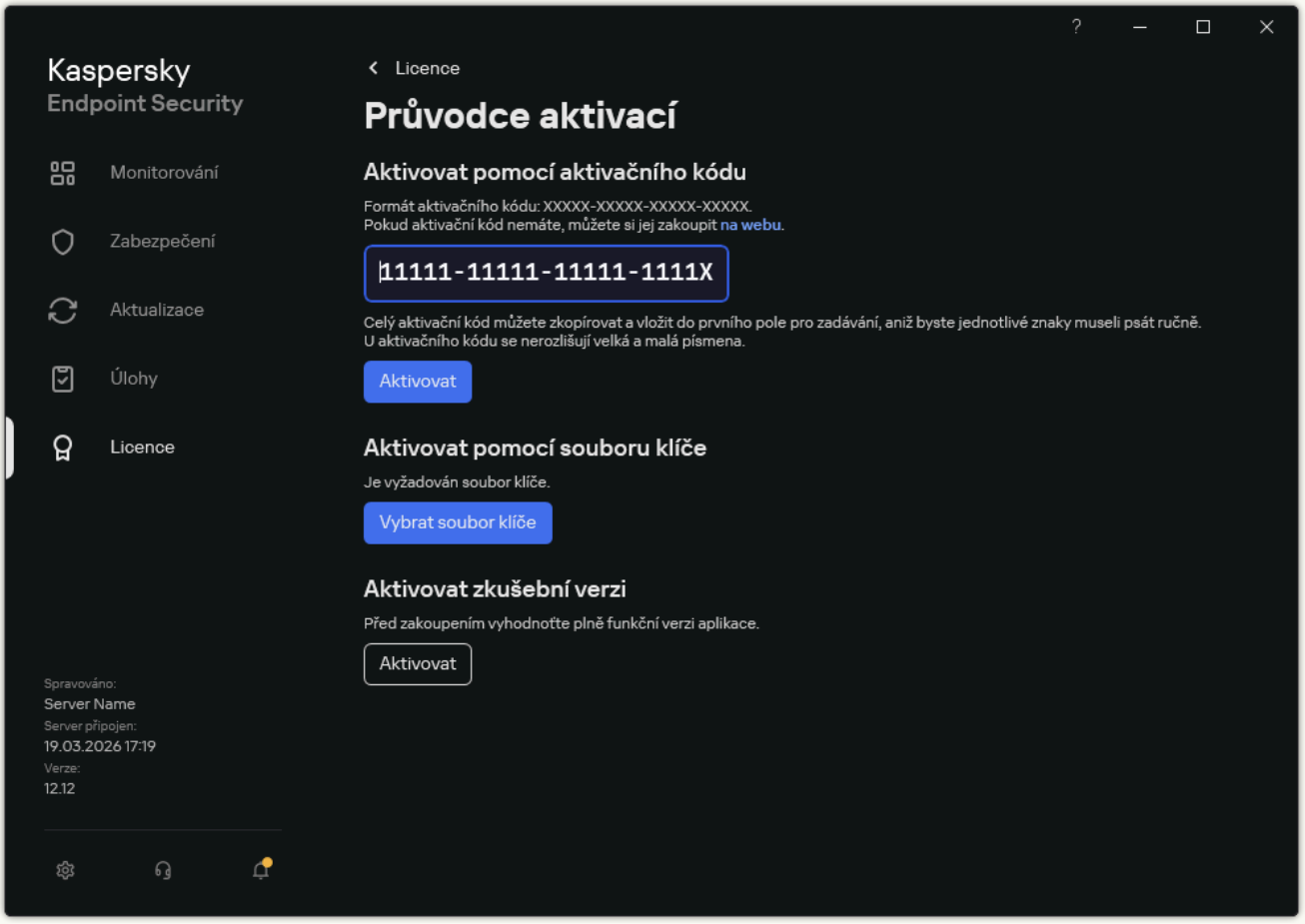
Krok 4. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Finish** 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.

Jak aktivovat aplikaci v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Licence**.
2. Klikněte na tlačítko **Aktivovat aplikaci pomocí nové licence**.

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



Aktivace aplikace

Ve vlastnostech úlohy *Přidání klíče* 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 **Kaspersky Licenses**.

   Otevře se seznam licenčních klíčů.
2. Otevřete vlastnosti licenčního klíče.
3. V části **General** zaškrtněte políčko **Automatically distribute license key to managed devices**.
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 **Devices** 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 konzoly vyberte možnosti **Operations** → **Licensing** → **Licenses**.
   Otevře se seznam licenčních klíčů.
2. Otevřete vlastnosti licenčního klíče.
3. Na kartě **General** zapněte přepínací tlačítko **Automatically distribute license key to managed devices**.
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 **Devices** můžete zobrazit počet počítačů, do kterých byl přidán klíč, a další data ve vlastnostech klíče.

Při aktivaci aplikace pomocí *aktivačního kódu* je vyžadován přístup k internetu pro připojení k aktivačním serverům Kaspersky. Pokud aplikaci aktivujete pomocí *souboru klíče*, není nutný přístup k internetu. Pokud jsou počítače v izolovaném segmentu sítě bez přístupu k internetu, musíte pro aktivaci aplikace pomocí kódu povolit použití serveru pro správu Kaspersky Security Center jako proxy serveru. To znamená, že aplikace může získat přístup k aktivačním serverům prostřednictvím serveru pro správu, který má přístup k internetu.

Jak povolit použití serveru pro správu jako proxy serveru pro aktivaci aplikace v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. Zaškrtněte políčko **Použít Kaspersky Security Center jako proxy server pro aktivaci**.
5. Uložte změny.

Jak povolit použití serveru pro správu jako proxy serveru pro aktivaci aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **KSC Integration**.
5. Zaškrtněte políčko **Use Kaspersky Security Center as proxy server for activation**.
6. Uložte změny.

Pokud nemůžete aplikaci aktivovat pomocí *aktivačního kódu*, můžete zkusit získat *soubor klíče* pomocí řešení Kaspersky a pokusit se aplikaci znovu aktivovat jiným způsobem.

Sledování využití licencí

Použití licencí můžete sledovat následujícími způsoby:

- Zobrazte možnost *Report on usage of license keys* pro infrastrukturu organizace (**Monitoring** → **Reports**).
- Zobrazte stavy počítačů na kartě **Managed devices** → **Devices**. Pokud aplikace není aktivována, počítač bude ve stavu ⚠ *Aplikace není aktivována*.
- Zobrazte informace o licenci ve vlastnostech.
- Zobrazte vlastnosti klíče (**Operations** → **Licensing**).

Specifika aktivace aplikace jako součásti cloudové konzoly aplikace 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.

Odebírání licenčního klíče

Chcete-li odebrat licenční klíč, musíte v počítačích spustit zvláštní úlohu. Licenční klíč můžete odebrat, například za účelem změny uspořádání jednotek licencování. Po skončení platnosti licence vás aplikace Kaspersky Endpoint Security upozorní také. Pokud jste přidali licenční klíč s krátkou dobou platnosti za účelem vyzkoušení aplikace (například doplněk EDR Optimum), můžete tento licenční klíč odebrat, abyste se zbavili upozornění a opravili stav svého počítače.

Úloha *Odstranit klíč* umožňuje odebrat z počítače všechny licenční klíče. Odebrat můžete aktivní i rezervní licenční klíče. Kromě aktivačního licenčního klíče aplikace Kaspersky Endpoint Security můžete odebrat jednotlivé licenční klíče řešení Detection and Response (například doplněk EDR Optimum).

Jak odebrat licenční klíč v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Odstranit klíč**.

Krok 2. Výběr licence

Vyberte licenční klíč, které chcete odstranit. Licenční klíč můžete vybrat z úložiště klíčů aplikace Kaspersky Security Center nebo vybrat soubor klíče.

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 *Odebrání klíče pro beta verzi*.

Krok 6. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak odebrat licenční klíč ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Remove key**.
3. Do pole **Task name** zadejte krátký popis, například *Odebrání klíče pro beta verzi*.
4. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy. Přejděte k dalšímu kroku.

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

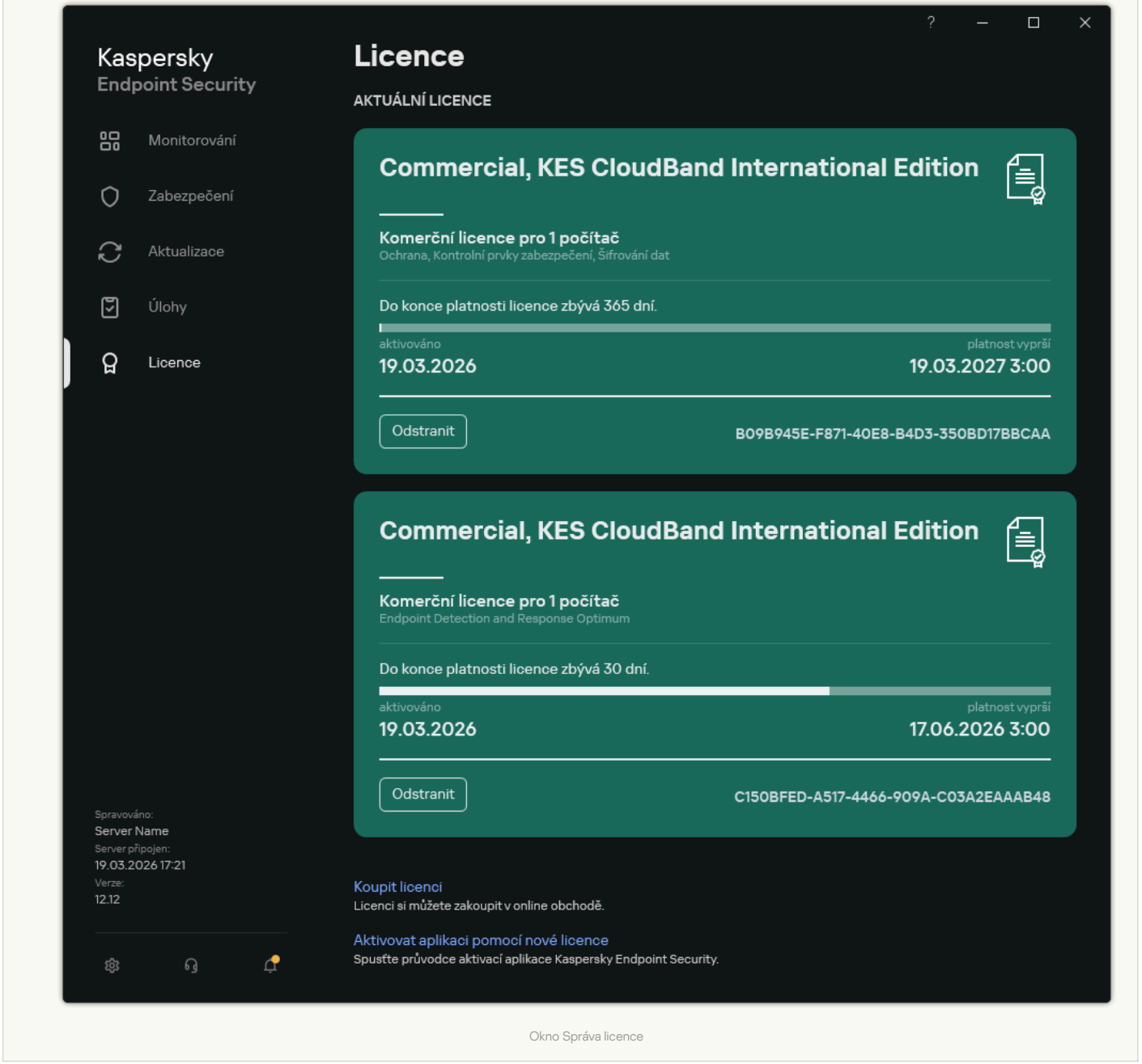
Vyberte licenční klíč, které chcete odstranit. Licenční klíč můžete vybrat z úložiště klíčů aplikace Kaspersky Security Center nebo vybrat soubor klíče. Přejděte k dalšímu kroku.

Krok 4. Dokončení vytvoření úlohy

Kliknutím na tlačítko **Finish** dokončete průvodce. V seznamu úloh se zobrazí nová úloha. Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**.

[Jak odebrat licenční klíč v rozhraní aplikace]

1. V hlavním okně aplikace přejděte do části **Licence**.
2. Vyberte klíč, který chcete odstranit, a klikněte na možnost **Odstranit**.



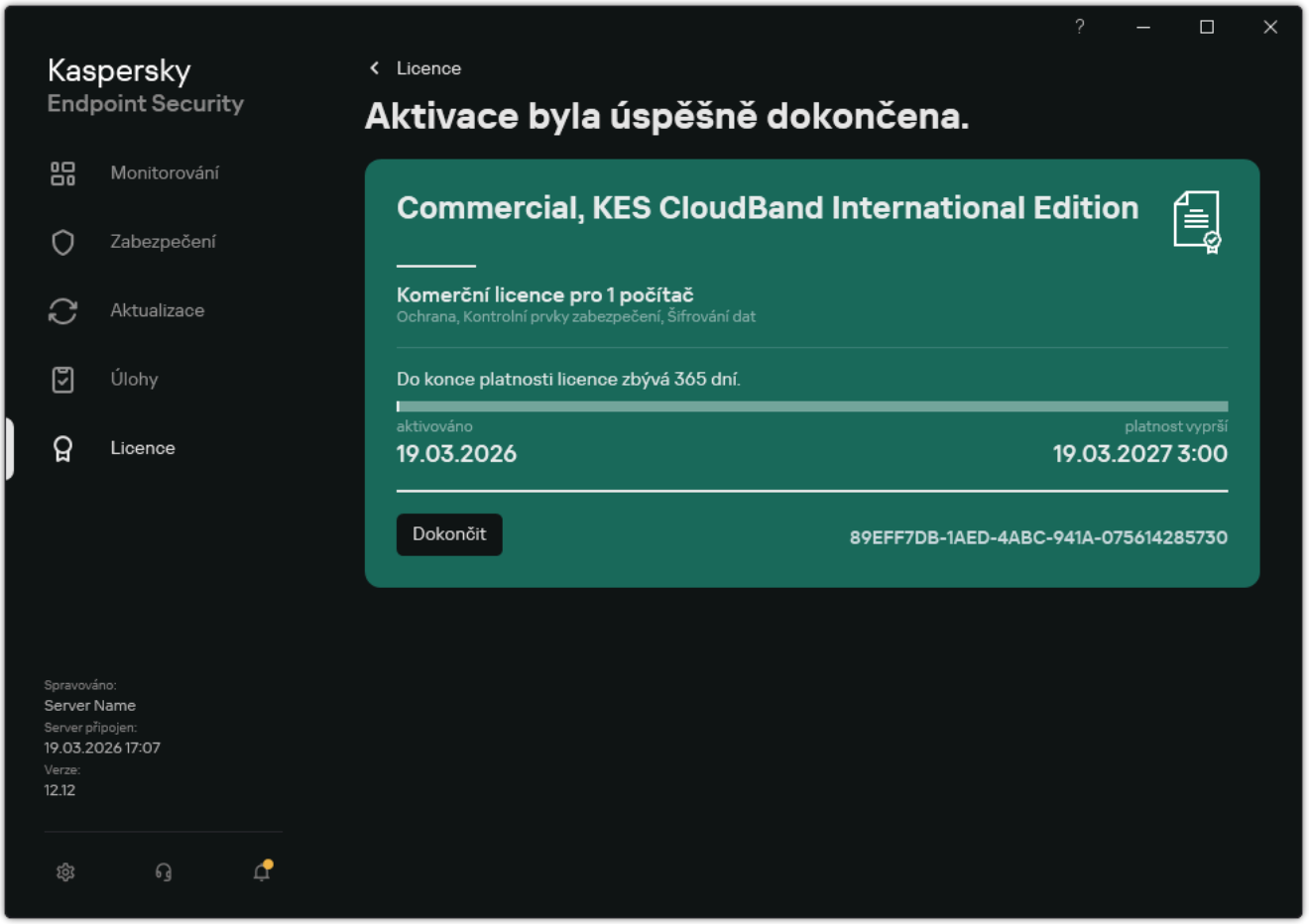
Okno Správa licence

Také můžete odebrat licenční klíč na příkazovém řádku.

Zobrazení informací o licenci

Postup zobrazení informací o licenci:

V hlavním okně aplikace přejděte na část **Licence** (viz obrázek níže).



Okno Správa licence

V této části se zobrazují následující údaje:

- *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 kliknutím na tlačítko **Odstranit**.
- *Název aplikace*. Úplný název zakoupené aplikace společnosti Kaspersky.
- *Typ licence*. K dispozici jsou následující typy licencí: zkušební a komerční.
- *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*. Datum počátku a konce licenčního období (pouze pro aktivní klíč), zbývající doba licenčního období.

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

- *Klíč*. Klíč je jedinečná alfanumerická série, která je vygenerována z aktivačního kódu nebo souboru klíče.

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

- **Koupit 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.
- **Aktivovat aplikaci pomocí nové licence**. 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 přejděte do části **Licence**.
2. Proveďte jednu z následujících akcí:

- Pokud nebyly přidány žádné klíče nebo byl přidán klíč zkušební licence, klikněte na tlačítko **Koupit 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.

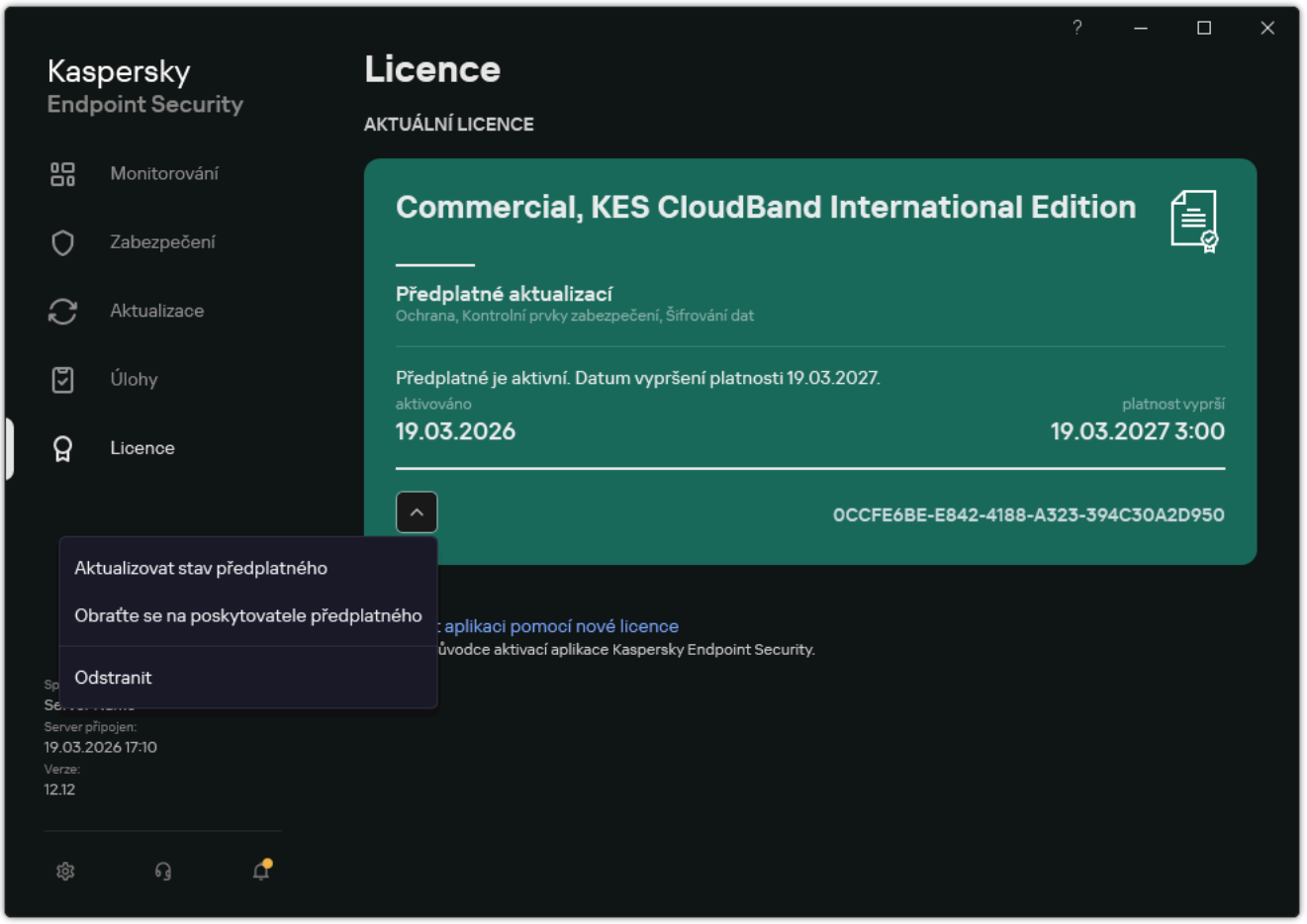
Pokud aplikaci používáte v rámci omezeného předplatného, v datu vypršení platnosti předplatného (nebo v datu vypršení platnosti lhůty pro obnovení předplatného) vás aplikace Kaspersky Endpoint Security na tuto skutečnost upozorní a již se nebude pokoušet o automatické obnovení předplatného. V tomto případě 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.

Navštívení webových stránek poskytovatele služeb prostřednictvím rozhraní aplikace:

1. V hlavním okně aplikace přejděte do části **Licence**.
2. Klikněte na tlačítko **Obraťte se na poskytovatele předplatného**.

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



Obnovení předplatného

Poskytování údajů

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);
- jedinečné ID požadavku na služby držitele práv;
- 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 aktuální licencí;
  - aktivní klíč;
  - licenční období aplikace Kaspersky Endpoint Security;
  - aktuální stav licence;

- typ aktuální 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 o Kaspersky Security Network. Soubory license.txt a ksn_<ID jazyka>.txt obsahují text licenční smlouvy s koncovým uživatelem a prohlášení o 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 o Kaspersky Security Network 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 o Kaspersky Security Network souhlasíte s automatickým přenesením těchto informací:

Pokud je zaškrtnuto políčko **Kaspersky Security Network** a není zaškrtnuto políčko **Povolit rozšířený režim 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 **Povolit rozšířený režim 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, SHA2-256, 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 skupina důvěryhodnosti, 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 Filelo / Disklo / 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.

Poskytování dat při používání řešení Detection and Response

Na počítačích s nainstalovanou aplikací Kaspersky Endpoint Security jsou data připravena k automatickému odeslání na servery Kaspersky Endpoint Detection and Response, Kaspersky Sandbox a Kaspersky Anti Targeted Attack Platform uložena. Soubory jsou uloženy na počítačích v prosté, nešifrované podobě.

Konkrétní sada dat závisí na řešení, v rámci kterého se aplikace Kaspersky Endpoint Security používá.

Kaspersky Endpoint Detection and Response

Při odinstalaci aplikace Kaspersky Endpoint Security jsou z počítače odstraněna všechna data, která aplikace ukládá lokálně v počítači.

Data přijatá jako výsledek provedení úlohy IOC Scan (standardní úloha)

Aplikace Kaspersky Endpoint Security automaticky odesílá data o výsledcích provedení úlohy *Kontrola IOC* do aplikace Kaspersky Security Center.

Data o výsledcích provádění úlohy *Kontrola IOC* mohou obsahovat následující informace:

- IP adresa z tabulky ARP
- Fyzická adresa z tabulky ARP
- Typ a název DNS záznamu

- IP adresa chráněného počítače
- Fyzická adresa (MAC adresa) chráněného počítače
- Identifikátor v položce protokolu událostí
- Název zdroje dat v protokolu
- Název protokolu
- Čas události
- Hodnoty hash MD5 a SHA256 souboru
- Celý název souboru (včetně cesty)
- Velikost souboru
- Vzdálená IP adresa a port, ke kterým bylo navázáno spojení během kontroly
- IP adresa místního adaptéru
- Otevřený port na místním adaptéru
- Protokol jako číslo (v souladu se standardem IANA)
- Název procesu
- Argumenty procesu
- Cesta k souboru procesu
- Identifikátor procesu v systému Windows (PID)
- Identifikátor nadřazeného procesu v systému Windows (PID)
- Uživatelský účet, který spustil proces
- Datum a čas, kdy byl proces zahájen
- Název služby
- Popis služby
- Cesta a název služby DLL (pro svchost)
- Cesta a název spustitelného souboru služby
- Identifikátor služby v systému Windows (PID)
- Typ služby (například ovladač jádra nebo adaptér)
- Stav služby
- Režim spuštění služby
- Název uživatelského účtu
- Název svazku
- Písmeno svazku
- Typ svazku
- Hodnota registru systému Windows
- Hodnota podregistru registru
- Cesta klíče registru (bez podregistru a názvu hodnoty)
- Nastavení registru
- Systém (prostředí)

- Název a verze operačního systému nainstalovaného v počítači
- Název sítě chráněného počítače
- Doména nebo skupina, do které chráněný počítač patří
- Název prohlížeče
- Verze prohlížeče
- Čas, kdy byl webový zdroj naposledy otevřen
- URL z požadavku HTTP
- Název účtu použitého pro požadavek HTTP
- Název souboru procesu, který provedl požadavek HTTP
- Úplná cesta k souboru procesu, který provedl požadavek HTTP
- Identifikátor procesu v systému Windows (PID), který provedl požadavek HTTP
- HTTP odkazujícího serveru (URL zdroje požadavku HTTP)
- URI zdroje požadovaného přes HTTP
- Informace o uživatelském agentovi HTTP (aplikace, která provedla požadavek HTTP)
- Doba provedení požadavku HTTP
- Jedinečný identifikátor procesu, který zadal dotaz HTTP

Data pro vytvoření řetězce vývoje hrozeb

Data pro vytvoření řetězce vývoje hrozeb se ve výchozím nastavení ukládají po dobu sedmi dnů. Data jsou automaticky odeslána do aplikace Kaspersky Security Center.

Data pro vytvoření řetězce vývoje hrozeb mohou obsahovat následující informace:

- Datum a čas události
- Název detekce
- Režim kontroly
- Stav poslední akce související s detekcí
- Důvod, proč se zpracování detekce nezdařilo
- Zjištěný typ objektu
- Zjištěný název objektu
- Stav ohrožení po zpracování objektu
- Důvod, proč se nezdařilo provádění akcí na objektu
- Akce provedené za účelem vrácení škodlivých akcí
- Informace o zpracovávaném objektu:
  - Jedinečný identifikátor procesu
  - Jedinečný identifikátor nadřazeného procesu
  - Jedinečný identifikátor souboru procesu
  - Identifikátor procesu v systému Windows (PID)
  - Příkazový řádek procesu
  - Uživatelský účet, který spustil proces

- Kód přihlašovací relace, ve které proces běží
- Typ relace, ve které proces běží
- Úroveň integrity zpracovávaného procesu
- Členství uživatelského účtu, který spustil proces, v místních skupinách a skupinách domény s oprávněním
- Identifikátor zpracovávaného objektu
- Celý název zpracovávaného objektu
- Identifikátor chráněného zařízení
- Celý název objektu (místní název souboru nebo webová adresa staženého souboru)
- Hodnota hash MD5 nebo SHA256 zpracovávaného objektu
- Typ zpracovávaného objektu
- Datum vytvoření zpracovávaného objektu
- Datum, kdy byl zpracovávaný objekt naposledy upraven
- Velikost zpracovávaného objektu
- Atributy zpracovávaného objektu
- Organizace, která podepsala zpracovávaný objekt
- Výsledek ověření digitálního certifikátu zpracovávaného objektu
- Bezpečnostní identifikátor (SID) zpracovávaného objektu
- Identifikátor časové zóny zpracovávaného objektu
- Webová adresa stahování zpracovávaného objektu (pouze pro soubory na disku)
- Název aplikace, která soubor stáhla
- Hodnoty hash MD5 a SHA256 aplikace, která soubor stáhla
- Název aplikace, která naposledy soubor upravila
- Hodnoty hash MD5 a SHA256 aplikace, která naposledy soubor upravila
- Počet spuštění zpracovávaného objektu
- Datum a čas, kdy byl zpracovávaný objekt poprvé spuštěn
- Jedinečné identifikátory souboru
- Celý název souboru (místní název souboru nebo webová adresa staženého souboru)
- Cesta ke zpracovávané proměnné registru Windows
- Název zpracovávané proměnné registru Windows
- Hodnota zpracovávané proměnné registru Windows
- Typ zpracovávané proměnné registru Windows
- Indikátor členství zpracovávaného klíče registru v bodě automatického spuštění
- Webová adresa zpracovávaného webového požadavku
- Zdroj odkazu zpracovávaného webového požadavku
- Uživatelský agent zpracovávaného webového požadavku
- Typ zpracovávaného webového požadavku (`GET` nebo `POST`)
- Místní IP port zpracovávaného webového požadavku

- Vzdálený IP port zpracovávaného webového požadavku
- Směr připojení (příchozí nebo odchozí) zpracovávaného webového požadavku
- Identifikátor procesu, do kterého byl škodlivý kód vložen

Kaspersky Sandbox

Při odinstalaci aplikace Kaspersky Endpoint Security jsou z počítače odstraněna všechna data, která aplikace ukládá lokálně v počítači.

Servisní data

Kaspersky Endpoint Security ukládá následující data zpracovávaná během automatické odpovědi:

- Zpracovávané soubory a data zadaná uživatelem během konfigurace integrovaného agenta Kaspersky Endpoint Security:
  - Soubory v karanténě
  - Veřejný klíč certifikátu použitý pro integraci s řešením Kaspersky Sandbox
- Mezipaměť integrovaného agenta Kaspersky Endpoint Security:
  - Čas, kdy byly výsledky kontroly zapsány do mezipaměti
  - MD5 hash úlohy kontroly
  - Identifikátor úlohy kontroly
  - Výsledek kontroly objektu
- Fronta požadavků na kontrolu objektů:
  - ID objektu ve frontě
  - Čas, kdy byl objekt umístěn do fronty
  - Stav zpracování objektu ve frontě
  - ID uživatelské relace v operačním systému, kde byla vytvořena úloha kontroly objektů
  - Systémový identifikátor (SID) uživatele operačního systému, jehož účet byl použit k vytvoření úlohy
  - MD5 hash úlohy kontroly objektů
- Informace o úlohách, pro které integrovaný agent Kaspersky Endpoint Security očekává výsledky kontroly z řešení Kaspersky Sandbox:
  - Čas, kdy byla přijata úloha kontroly objektů
  - Stav zpracování objektu
  - ID uživatelské relace v operačním systému, kde byla vytvořena úloha kontroly objektů
  - Identifikátor úlohy kontroly objektů
  - MD5 hash úlohy kontroly objektů
  - Systémový identifikátor (SID) uživatele operačního systému, jehož účet byl použit k vytvoření úlohy
  - XML schéma automaticky vytvořeného IOC
  - Hodnota hash MD5 nebo SHA256 kontrolovaného objektu
  - Chyba zpracování
  - Názvy objektů, pro které byla úloha vytvořena
  - Výsledek kontroly objektu

Údaje v požadavcích na Kaspersky Sandbox

Následující data z požadavků od integrovaného agenta Kaspersky Endpoint Security na Kaspersky Sandbox jsou uložena lokálně v počítači:

- MD5 hash úlohy kontroly
- Identifikátor úlohy kontroly
- Kontrolovaný objekt a všechny související soubory

Data přijatá jako výsledek provedení úlohy IOC Scan (samostatná úloha)

Aplikace Kaspersky Endpoint Security automaticky odesílá data o výsledcích provedení úlohy *Kontrola IOC* do aplikace Kaspersky Security Center.

Data o výsledcích provádění úlohy *Kontrola IOC* mohou obsahovat následující informace:

- IP adresa z tabulky ARP
- Fyzická adresa z tabulky ARP
- Typ a název DNS záznamu
- IP adresa chráněného počítače
- Fyzická adresa (MAC adresa) chráněného počítače
- Identifikátor v položce protokolu událostí
- Název zdroje dat v protokolu
- Název protokolu
- Čas události
- Hodnoty hash MD5 a SHA256 souboru
- Celý název souboru (včetně cesty)
- Velikost souboru
- Vzdálená IP adresa a port, ke kterým bylo navázáno spojení během kontroly
- IP adresa místního adaptéru
- Otevřený port na místním adaptéru
- Protokol jako číslo (v souladu se standardem IANA)
- Název procesu
- Argumenty procesu
- Cesta k souboru procesu
- Identifikátor procesu v systému Windows (PID)
- Identifikátor nadřazeného procesu v systému Windows (PID)
- Uživatelský účet, který spustil proces
- Datum a čas, kdy byl proces zahájen
- Název služby
- Popis služby
- Cesta a název služby DLL (pro svchost)
- Cesta a název spustitelného souboru služby
- Identifikátor služby v systému Windows (PID)
- Typ služby (například ovladač jádra nebo adaptér)
- Stav služby

- Režim spuštění služby
- Název uživatelského účtu
- Název svazku
- Písmeno svazku
- Typ svazku
- Hodnota registru systému Windows
- Hodnota podregistru registru
- Cesta klíče registru (bez podregistru a názvu hodnoty)
- Nastavení registru
- Systém (prostředí)
- Název a verze operačního systému nainstalovaného v počítači
- Název sítě chráněného počítače
- Doména nebo skupina, do které chráněný počítač patří
- Název prohlížeče
- Verze prohlížeče
- Čas, kdy byl webový zdroj naposledy otevřen
- URL z požadavku HTTP
- Název účtu použitého pro požadavek HTTP
- Název souboru procesu, který provedl požadavek HTTP
- Úplná cesta k souboru procesu, který provedl požadavek HTTP
- Identifikátor procesu v systému Windows (PID), který provedl požadavek HTTP
- HTTP odkazujícího serveru (URL zdroje požadavku HTTP)
- URl zdroje požadovaného přes HTTP
- Informace o uživatelském agentovi HTTP (aplikace, která provedla požadavek HTTP)
- Doba provedení požadavku HTTP
- Jedinečný identifikátor procesu, který zadal dotaz HTTP

Kaspersky Endpoint Detection and Response Expert (on-premise)

Při odinstalaci aplikace Kaspersky Endpoint Security jsou z počítače odstraněna všechna data, která aplikace ukládá lokálně v počítači.

Servisní data

Integrovaný agent Kaspersky Endpoint Security lokálně ukládá následující data:

- Data nutná pro integraci se součástí EDR Expert (on-premise):
  - Adresa a port pro připojení k serveru Central Node KATA
  - Adresa a port pro připojení k serveru pro přenos telemetrie
  - Adresa a port pro připojení k odpovědnímu serveru
  - Informace o certifikátech použitých pro integraci se serverem Central Node KATA
  - Informace o certifikátech použitých pro integraci se serverem pro přenos telemetrie

- Informace o certifikátech použitých pro integraci s odpovědním serverem

- Soubory v karanténě

Data z přenášených událostí telemetrie

- Telemetrická data

  - Údaje o souborech:
    - Jedinečné identifikátory souboru
    - Typ souboru
    - Úplná cesta ke zdrojovému souboru
    - Velikost souboru
    - Atributy souboru
    - Identifikátor zóny
    - Datum a čas, kdy byl soubor vytvořen
    - Datum a čas, kdy byl soubor naposledy upraven
    - Původní název souboru
    - Název aplikace
    - Verze aplikace
    - Dodavatel aplikace
    - Popis souboru
    - Verze souboru
    - Hodnoty hash MD5 a SHA256 objektu
    - Výsledek ověření podpisu souboru
    - Název vydavatele certifikátu
    - Jméno držitele certifikátu
    - Sériové číslo certifikátu
  - Údaje o kontrole AMSI:
    - Jedinečný identifikátor procesu, který inicioval příslušnou aktivitu
    - Typ obsahu objektu předaného do AMSI
    - Obsah objektu předaného do AMSI
    - Název objektu
    - Hodnoty hash MD5 a SHA256 objektu
  - Údaje o blokování aplikace:
    - Jedinečný identifikátor procesu, který inicioval blokování aplikace
    - Jedinečný identifikátor nadřazeného procesu
    - Jedinečný identifikátor procesu v systému
    - Příkaz použitý ke spuštění procesu
    - ID relace přihlášení

    - Úroveň integrity procesu
    - Stav procesu
    - Jedinečný identifikátor souboru procesu
    - Příkazový řádek procesu
    - Seznam jedinečných identifikátorů interpretovaných souborů
- Údaje o zablokovaných otevřeních souborů:
    - Jedinečný identifikátor procesu, který inicioval otevření souboru
    - Jedinečné identifikátory souboru
- Údaje o načítání ovladače:
    - Jedinečný identifikátor načteného ovladače
- Údaje o událostech:
    - Jedinečný identifikátor události
    - Datum a čas události
- Údaje o úpravě souboru:
    - Jedinečný identifikátor procesu, který inicioval úpravu souboru
    - Jedinečné identifikátory souboru
    - Typ operace úpravy
    - Příznak označující, že soubor bude po restartování počítače odstraněn
    - Jedinečný identifikátor upraveného souboru
    - Jedinečný identifikátor souboru před úpravou
    - Sada bitových příznaků, které určují způsob otevření souboru
    - Údaje o operacích na seznamu řízení přístupu
    - Údaje o změnách vlastnictví nebo nadřazené skupiny souboru
- Údaje o relaci přihlášení:
    - ID relace přihlášení
    - Jméno uživatele, který se přihlásil
    - Typ uživatelského účtu
    - Typ relace
- Údaje o síťových připojeních:
    - Jedinečný identifikátor procesu, který navázal připojení
    - Místní IP adresa použitá k navázání připojení
    - Vzdálená IP adresa koncového bodu připojení
    - Směr připojení
    - Protokol přenosu dat
    - Metoda HTTP
    - Cesta bez názvu hostitele
    - Název hostitele

- Dynamický stav procesu v okamžiku připojení
- Příznak označující, že je připojení otevřené na úrovni nezpracovaného soketu
- Verze TLS použitá v relaci připojení
- Název serveru TLS
- Hodnoty hash MD5 a SHA1 certifikátu serveru TLS
- Seznam alternativních názvů předmětu (SAN) certifikátu
- Název vydavatele certifikátu TLS
- Sériové číslo certifikátu
- Použitý šifrovací algoritmus
- Datum zahájení a ukončení certifikátu
- Digitální otisk JA3 klienta TLS
- Digitální otisk serveru JA3S

- Data zachycená při poslechu na síťovém portu:
  - Jedinečný identifikátor procesu, který navázal připojení
- Vstupní data příkazového řádku:
  - Jedinečný identifikátor procesu, který inicioval vstup konzoly
  - Typ vstupu konzoly
  - Text zadaný uživatelem nebo procesem
- Údaje o vytvoření procesu:
  - Jedinečný identifikátor procesu
  - Jedinečný identifikátor nadřazeného procesu
  - Jedinečný identifikátor procesu v systému
  - Příkaz použitý ke spuštění procesu
  - ID relace přihlášení
  - Úroveň integrity procesu
  - Jedinečný identifikátor souboru procesu
  - Seznam jedinečných identifikátorů interpretovaných souborů
  - Typ procesu
- Údaje o modulu načteném procesem:
  - Jedinečný identifikátor procesu, který inicioval stahování
  - Úplná cesta k souboru, který byl nahrán do procesu
  - Jedinečný identifikátor souboru modulu
  - Úplný kvalifikovaný název sestavení .NET, pokud je načítaným souborem modul .NET
  - Příznaky sestavení .NET definované v jeho souboru manifest
- Údaje o ukončení procesu:
  - Jedinečný identifikátor ukončeného procesu
- Údaje o změně registru:

- Jedinečný identifikátor procesu, který inicioval změnu registru
- Typ operace registru
- Úplná cesta ke klíči registru
- Název hodnoty v rámci klíče registru
- Typ dat uložených v hodnotě klíče registru
- Data zadaná v hodnotě klíče registru
- Název klíče před přejmenováním
- Informace týkající se změny vlastnictví klíče nebo skupiny primárních klíčů
- Seznam změn v seznamu řízení přístupu (ACL) klíče

- Údaje o zjištěné hrozbě a jejím zpracování:
  - Příznak označující, že zjišťování hrozeb bylo spuštěno na pozadí
  - Verdikt ohledně hrozby
  - Název verdiktu
  - Jedinečný identifikátor záznamu v databázi
  - Čas, kdy byl záznam o hrozbě uložen do databáze
  - Režim zpracování hrozby
  - Typ infikovaného objektu
  - Název infikovaného objektu
  - Hodnoty hash MD5 a SHA256 objektu
  - Jedinečný identifikátor infikovaného objektu
  - Jedinečný identifikátor procesu, který stáhl infikovaný objekt z internetu
  - Adresa URL, ze které byl infikovaný objekt stažen
  - E-mailová adresa odesílatele, která odeslala infikovaný objekt
  - Síťový protokol, jehož prostřednictvím byl infikovaný objekt přijat
  - Místní adresa, ze které byl infikovaný objekt přijat
  - Externí adresa, ze které byl infikovaný objekt přijat
  - Typ obsahu objektu
  - Obsah objektu
- Údaje o přístupu k procesům:
  - Jedinečný identifikátor procesu, který se pokusil o přístup
  - Jedinečný identifikátor cílového procesu, ke kterému proces přistupoval
  - Sada práv požadovaná od cílového procesu
  - Typ operace
  - Sada volání v okamžiku přístupu k procesu
  - Deskriptor zdrojového procesu
  - Deskriptor cílového procesu
- Údaje o DNS:

- Jedinečný identifikátor procesu, který inicioval dotaz DNS
- IP adresa serveru DNS
- Příznaky, které spravují chování dotazu DNS
- Stav provádění požadavku
- Úplný název domény zadaný v dotazu DNS
- Datový typ v dotazu DNS
- Odpovědi serveru DNS

- Údaje o vložení kódu:
  - Jedinečný identifikátor procesu, který se pokusil o vložení kódu
  - Použitý způsob přístupu
  - Sada volání v době, kdy byl vložený kód detekován
  - Jedinečný identifikátor cílového procesu, do kterého byl kód vložen
  - Údaje o změnách v příkazové sekvenci cílového procesu
  - Adresa cílového procesu
  - Název knihovny DLL, která byla nahrána do cílového procesu
  - Úplná cesta k souboru DDL
- Údaje o operacích s pojmenovanými kanály:
  - Jedinečný identifikátor procesu, který vytvořil kanál nebo se k němu připojil
  - Úplný název pojmenovaného kanálu
  - Typ operace (vytvoření nebo připojení)
- Údaje o dotazech WMI:
  - Jedinečný identifikátor procesu, který inicioval operaci WMI
  - Typ operace WMI
  - Název cílového zařízení pro dotaz WMI
  - Uživatelský účet, který zadal dotaz WMI
  - Text dotazu WMI
  - Obor názvů, ve kterém se provádí dotaz WMI
  - Název filtru WMI
  - Název objektu uživatele
  - Text popisující akci objektu uživatele
- Údaje o dotazech LDAP:
  - Jedinečný identifikátor procesu, který zadal dotaz LDAP
  - Rozsah hledání dotazů LDAP
  - Filtr LDAP
  - Parametr určující oddíl služby Active Directory, na který byl dotaz přesměrován
  - Atributy hledání LDAP
- Údaje o připojených zařízeních USB:

- Typ provozu zařízení USB
- Typ zařízení USB
- Identifikátor zařízení USB
- Název zařízení USB
- Cesta k zařízení USB
- Příznak označující, že zařízení USB je systémová jednotka

- Údaje o vytvoření, odstranění a úpravě naplánované úlohy
- Údaje o vytvoření, odstranění a úpravě služeb
- Údaje o připojení/odpojení souborového systému
- Údaje o provozu místní součásti EDR Expert:
  - Informace o spuštění/zastavení agenta
  - Informace o instalaci/odinstalaci agenta
  - Jedinečný identifikátor pro spuštění agenta
  - Systémový identifikátor procesu agenta
  - Jedinečný identifikátor procesu agenta
  - Důvod ukončení agenta
  - Kód ukončení procesu agenta

- Nastavení filtrování událostí:
  - Název modulu
  - Úplné cesty k objektům
  - Hodnoty hash MD5 a SHA256 objektů
  - Identifikátory položek v protokolu událostí systému Windows
  - Nastavení digitálního certifikátu
  - Směr provozu, IP adresy, porty, protokoly, úplné cesty ke spustitelným souborům
  - Uživatelské jméno
  - Typy přihlášení uživatele
  - Typy telemetrických událostí, pro které jsou použity filtry

Data z požadavků součásti EDR Expert na integrovaného agenta Kaspersky Endpoint Security

- Obecné nastavení úlohy:
  - Typ úlohy
  - Nastavení plánu úloh
  - Jména a hesla účtů, pod kterými lze úlohy spouštět
  - Verze nastavení
  - Identifikátory objektů v karanténě
  - Cesty k objektům
  - Hodnoty hash MD5 a SHA256 objektů

- Příkazový řádek pro spuštění procesu s argumenty
- Příznaky dalších akcí provedených po dokončení úloh
- Identifikátory souborů IOC, které mají být načteny ze serveru
- Soubory IOC
- Název služby
- Typ spuštění služby
- Složky, pro které musí být obdrženy výsledky úlohy *Načíst forenzní údaje*
- Masky názvů objektů a rozšíření pro úlohu *Načíst forenzní údaje*

- Nastavení izolace sítě:
  - Typy nastavení
  - Verze nastavení
  - Seznamy výjimek z izolace sítě a nastavení výjimek: směr provozu, IP adresy, porty, protokoly a úplné cesty ke spustitelným souborům
  - Příznaky dalších akcí
  - Doba deaktivace automatické izolace
- Nastavení prevence spouštění:
  - Typy nastavení
  - Verze nastavení
  - Seznamy pravidel prevence spouštění a nastavení pravidel: cesty k objektům, typy objektů, hodnoty hash MD5 a SHA256 objektů
  - Příznaky dalších akcí

Data z požadavků zaslaných aplikací Kaspersky Endpoint Security do součásti EDR Expert

Při integraci s řešením EDR Expert (on-premise) se lokálně v počítačích ukládají následující data.

- V požadavcích na synchronizaci:
  - Jedinečné ID
  - Základní část webové adresy serveru
  - Název počítače
  - IP adresa počítače
  - MAC adresa počítače
  - Místní čas na počítači
  - Stav sebeobrany Kaspersky Endpoint Security
  - Název a verze operačního systému nainstalovaného v počítači
  - Verze aplikace Kaspersky Endpoint Security
  - Verze nastavení aplikace a nastavení úloh
  - Stavy úloh: identifikátory úloh, stavy provádění, kódy chyb
- V požadavcích na získání souborů ze serveru:
  - Jedinečné identifikátory souborů
  - Jedinečný identifikátor aplikace Kaspersky Endpoint Security
  - Jedinečné identifikátory certifikátů

- Základní část webové adresy serveru s nainstalovanou součástí Central Node
- IP adresa hostitele

- Ve zprávách o výsledcích provádění úlohy:
  - IP adresa hostitele
  - Informace o objektech zjištěných během kontroly IOC nebo kontroly YARA
  - Příznaky dalších akcí provedených po dokončení úloh
  - Chyby provádění úlohy a návratové kódy
  - Stavy dokončení úlohy
  - Čas dokončení úlohy
  - Verze nastavení použité pro provádění úloh
  - Informace o objektech odeslaných na server, objektech v karanténě a objektech obnovených z karantény: cesty k objektům, hodnoty hash MD5 a SHA256, identifikátory objektů v karanténě
  - Informace o procesech spuštěných nebo zastavených v počítači na žádost serveru: PID a UniquePID, kód chyby, hodnoty hash MD5 a SHA256 objektů
  - Informace o službách spuštěných nebo zastavených v počítači na žádost serveru: název služby, typ spouštění, kód chyby, hodnoty hash MD5 a SHA256 bitových kopií souborů služeb
  - Informace o objektech, pro které byl vytvořen výpis paměti pro kontrolu YARA (cesty, identifikátor souboru výpisu)
  - Soubory požadované serverem
- Údaje o běžících procesech:
  - Název spustitelného souboru včetně úplné cesty a přípony
  - Parametry automatického spuštění procesu
  - ID procesu
  - ID relace přihlášení
  - Přihlašovací jméno relace
  - Datum a čas, kdy byl proces zahájen
  - Hodnoty hash MD5 a SHA256 objektu
- Údaje o souborech:
  - Cesta k souboru
  - Název souboru
  - Velikost souboru
  - Atributy souboru
  - Datum a čas, kdy byl soubor vytvořen
  - Datum a čas, kdy byl soubor naposledy upraven
  - Popis souboru
  - Název společnosti
  - Hodnoty hash MD5 a SHA256 objektu
  - Klíč registru (pro body automatického spouštění)
- Data v chybách, ke kterým dochází při načítání informací o objektech:
  - Úplný název objektu, který byl zpracován, když došlo k chybě

- Kód chyby

- Data ve výsledcích kontroly YARA:

  Integrovaný agent Kaspersky Endpoint Security automaticky přenáší výsledky kontroly YARA na platformu Kaspersky Anti Targeted Attack Platform za účelem vytvoření řetězce vývoje hrozeb.

  Data jsou dočasně uložena lokálně ve frontě pro odesílání výsledků provádění úloh na server Kaspersky Anti Targeted Attack Platform. Po odeslání jsou data z dočasného úložiště odstraněna.

  - Hodnoty hash MD5 a SHA256 souboru
  - Celý název souboru
  - Cesta k souboru
  - Velikost souboru
  - Název procesu
  - Argumenty procesu
  - Cesta k souboru procesu
  - Identifikátor procesu v systému Windows (PID)
  - Identifikátor nadřazeného procesu v systému Windows (PID)
  - Uživatelský účet, který spustil proces
  - Datum a čas, kdy byl proces zahájen

- Data ve výsledcích kontroly IOC:

  - IP adresa z tabulky ARP
  - Fyzická adresa z tabulky ARP
  - Název záznamu DNS
  - Typ záznamu DNS
  - Název hostitele
  - IP adresa
  - ID události v protokolu
  - Název zdroje dat v protokolu
  - Název protokolu
  - Uživatelské jméno
  - Datum a čas vygenerování události ve formátu ISO
  - Hodnoty hash MD5 a SHA256 souboru
  - Celý název souboru
  - Velikost souboru
  - Vzdálená IP adresa a port, ke kterým bylo navázáno spojení během kontroly
  - IP adresa a port místního adaptéru
  - Protokol
  - Název procesu
  - Argumenty procesu
  - Cesta k souboru procesu
  - Identifikátor procesu v systému Windows (PID)

- Identifikátor nadřazeného procesu v systému Windows (PID)
- Uživatelský účet, který spustil proces
- Datum a čas, kdy byl proces zahájen
- Cesta ke klíči registru
- Název klíče registru
- Textová hodnota klíče registru
- Název služby
- Popis služby
- Cesta a název služby DLL
- Cesta a název spustitelného souboru služby
- Identifikátor služby v systému Windows (PID)
- Typ služby
- Stav služby
- Režim spuštění služby
- Název operačního systému
- Verze operačního systému
- Název počítačové sítě bez domény
- Doména nebo pracovní skupina
- Uživatelské jméno
- Název svazku
- Písmeno svazku
- Typ svazku

Kaspersky Network Detection and Response (KATA)

Při odinstalaci aplikace Kaspersky Endpoint Security jsou z počítače odstraněna všechna data, která aplikace ukládá lokálně v počítači.

Telemetrická data

- Údaje o souborech
  - Jedinečné identifikátory souboru
  - Typ souboru
  - Úplná cesta ke zdrojovému souboru
  - Velikost souboru
  - Atributy souboru
  - Identifikátor zóny
  - Datum a čas, kdy byl soubor vytvořen
  - Datum a čas, kdy byl soubor naposledy upraven
  - Původní název souboru

- Název aplikace
- Verze aplikace
- Dodavatel aplikace
- Popis souboru
- Verze souboru
- Hodnoty hash MD5 a SHA256 objektu
- Výsledek ověření podpisu souboru
- Datum a čas, kdy byl podpis souboru vytvořen
- Řetězce certifikátů použité v souboru podpisu
- Typ řetězce certifikátů
- Certifikáty v řetězci
- Název vydavatele certifikátu
- Jméno držitele certifikátu
- Sériové číslo certifikátu
- Algoritmus otisku certifikátu
- Otisk certifikátu
- Doba platnosti certifikátu

- Údaje o relaci přihlášení
  - ID relace přihlášení
  - Název účtu uživatele, který se přihlásil
  - Typ uživatelského účtu
  - Typ relace
  - IP adresa počítače, ze kterého byl proveden pokus o přihlášení
  - IP adresa místního počítače, u kterého byl proveden pokus o přihlášení
  - Příznak označující, že relace představovaná touto událostí má zvýšená oprávnění a oprávnění pro správu
  - Parametr označující, zda jsou s touto relací přihlášení spojeny další relace
  - Protokol použitý pro relaci terminálu
  - Protokol IPv4 použitý pro relaci terminálu
- Údaje o síťové komunikaci
  - Začátek a konec časového intervalu, za který byla data shromážděna
  - Seznam připojení
  - Místní IP adresa počítače
  - Místní MAC adresa počítače
  - Vzdálená IP adresa počítače

- Vzdálená MAC adresa počítače
- IP adresa brány
- Počet přenesených datových paketů
- Počet přijatých datových paketů
- Celkový počet přenesených bajtů
- Protokol přenosu dat
- Pole EtherType rámce sítě Ethernet
- Předpona datové části prvního paketu v intervalu
- IPv4 adresa síťového rozhraní, přes které byla komunikace zachycena

- Údaje o síťovém připojení
  - Jedinečný identifikátor procesu, který navázal připojení
  - Protokol přenosu dat
  - Místní IP adresa použitá k navázání připojení
  - Vzdálená IP adresa koncového bodu připojení
  - Metoda HTTP
  - Cesta bez názvu hostitele
  - Název hostitele
  - Dynamický stav procesu v okamžiku připojení
  - Směr připojení
  - Dynamický stav procesu
  - Pole EtherType rámce sítě Ethernet
- Data zachycená při poslechu na síťovém portu
  - Jedinečný identifikátor procesu, který navázal připojení
  - Protokol přenosu dat
  - Místní adresa
  - Dynamický stav procesu v okamžiku připojení
- Výsledek ověření připojení
  - Nastavení sítě hostitele
  - Popis síťového rozhraní
  - Název domény DNS
  - Místní MAC adresa počítače
  - Číslo metriky IP připojení
  - Seznam IP adres

- IP adresa
- Maska sítě
- IP adresa brány
- MAC adresa brány
- Seznam nainstalovaných oprav
- Číslo opravy
- Datum instalace opravy
- Model zařízení
- Výrobce zařízení
- ID hostitele v aplikaci Kaspersky Security Center
- Popis nainstalovaného antiviru Kaspersky
- Název součásti nainstalovaného antiviru Kaspersky
- Verze součásti nainstalovaného antiviru Kaspersky
- Verze databáze nainstalované antivirové součásti Kaspersky
- Datum poslední aktualizace databáze nainstalované antivirové součásti Kaspersky
- Stav součásti nainstalovaného antiviru Kaspersky
- Seznam licenčních klíčů
- Sériové číslo klíče
- Typ klíče
- Datum vypršení platnosti klíče
- Stav klíče

- **Údaje o vytváření procesu na hostiteli**

  - Jedinečný identifikátor procesu
  - Jedinečný identifikátor nadřazeného procesu
  - Jedinečný identifikátor procesu v systému
  - Příkaz použitý ke spuštění procesu
  - ID relace přihlášení
  - ID relace terminálu
  - Jedinečný identifikátor souboru procesu
  - Úroveň integrity procesu
  - Seznam tokenů práv procesů
  - Práva k atributům
  - Seznam jedinečných identifikátorů interpretovaných souborů
  - Stav procesu
  - Příkaz použitý ke spuštění procesu

- Údaje o ukončení procesu
  - Jedinečný identifikátor procesu
- Údaje o zjištěné hrozbě
  - Informace o hrozbě
  - Verdikt ohledně hrozby
  - Číslo záznamu AMR
  - Verze antivirové databáze
  - Režim detekce hrozeb
  - Jedinečný identifikátor hrozby
  - Technologie ochrany
  - Informace o infikovaném objektu
  - Typ infikovaného objektu
  - Název infikovaného objektu
  - Hodnoty hash MD5 a SHA256 objektu
  - Jedinečný identifikátor infikovaného procesu
  - Jedinečný identifikátor infikovaného objektu
  - Jedinečný identifikátor procesu, který stáhl infikovaný objekt z internetu
  - Adresa URL, ze které byl infikovaný objekt stažen
  - E-mailová adresa odesílatele, která odeslala infikovaný objekt
  - Síťový protokol, jehož prostřednictvím byl infikovaný objekt přijat
  - Místní adresa, ze které byl infikovaný objekt přijat
  - Externí adresa, ze které byl infikovaný objekt přijat
  - Typ obsahu objektu
  - Kontext zjištěné hrozby
  - Obsah objektu
  - Příznak označující, že zjišťování hrozeb bylo spuštěno na pozadí
- Údaje o zpracování hrozeb
  - Informace o hrozbě
  - Verdikt ohledně hrozby
  - Číslo záznamu AMR
  - Verze antivirové databáze
  - Režim detekce hrozeb
  - Název infikovaného objektu

- Hodnoty hash MD5 a SHA256 objektu
- Jedinečný identifikátor infikovaného procesu
- Jedinečný identifikátor infikovaného objektu
- Síťový protokol, jehož prostřednictvím byl infikovaný objekt přijat
- Místní adresa, ze které byl infikovaný objekt přijat
- Externí adresa, ze které byl infikovaný objekt přijat
- Stav zpracování hrozby
- Důvod, proč hrozbu nelze napravit
- Místní fyzická adresa

- **Údaje o uživatelích**
  - SID uživatele
  - ID uživatele
  - Uživatelské jméno
  - Celé jméno uživatele
  - Popis uživatele
  - Zda je účet aktivní nebo zablokovaný
  - Zda vypršela platnost hesla
  - Zda je nutná změna hesla
  - Zda je povolena změna hesla
  - Typ uživatelského účtu
  - Zda je pro tento účet povoleno automatické přihlašování
  - Seznam skupin, do nichž uživatel patří

Integrace s platformou Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Při odinstalaci aplikace Kaspersky Endpoint Security jsou z počítače odstraněna všechna data, která aplikace ukládá lokálně v počítači.

Při integraci s pplatformou Kaspersky Unified Monitoring and Analysis Platform (KUMA) jsou přenášena data nastavení připojení a také všechny události registrované v protokolech systému Windows.

Hlavní protokoly událostí systému Windows jsou System, Security, Application, ForwardedEvents a HardwareEvents. Uživatelé mohou také vytvářet vlastní protokoly a pracovat s nimi tak, aby splňovaly jejich konkrétní požadavky.

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

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 o 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 o Kaspersky Security Network. Soubory license.txt a ksn_<ID jazyka>.txt obsahují text licenční smlouvy s koncovým uživatelem a prohlášení o 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 o Kaspersky Security Network. Pokud nesouhlasíte s poskytováním těchto údajů společnosti Kaspersky, použijte službu Kaspersky Private Security Network (KPSN) nebo zakažte používání KSN. Více informací o KPSN naleznete v dokumentaci ke službě 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.
- 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 a cloudová konzola aplikace Kaspersky Security Center

Webová konzola aplikace Kaspersky Security Center (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 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 je poskytována prostřednictvím webového pluginu.

Verze modulu plug-in administrace se může lišit 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 ve webové konzole aplikace Kaspersky Security Center nainstalován. Webový modul plug-in musí být nainstalován v počítači, který má nainstalovanou webovou konzolu aplikace Kaspersky Security Center. Funkce webového modulu plug-in je k dispozici pro všechny správce, kteří mají přístup k webové konzoli v prohlížeči. V rozhraní webové konzoly můžete zobrazit seznam nainstalovaných webových modulů plug-in (**Console settings** → **Web plug-ins**). Podrobnější informace o kompatibilitě verzí webových modulů plug-in a webové konzole najdete v nápovědě k aplikaci Kaspersky Security Center.

Pokud používáte Kaspersky Endpoint Security jako součást řešení Kaspersky Endpoint Detection and Response Optimum, musíte nainstalovat modul plug-in pro správu řešení Kaspersky Endpoint Detection and Response. K zobrazení podrobností výstrahy potřebujete modul plug-in pro správu. *Podrobnosti o výsledcích detekce* je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. K vytváření úloh reakce na hrozby tedy potřebujete modul plug-in pro správu aplikace Kaspersky Endpoint Security a k zobrazení podrobností o výstrahách potřebujete modul plug-in pro správu EDR.

Instalace webového modulu plug-in

Webový modul plug-in lze nainstalovat následujícím způsobem:

- Nainstalujte webový modul plug-in pomocí průvodce Quick Start Wizard webové konzoly aplikace Kaspersky Security Center.

  Webová konzola vás automaticky vyzve, abyste průvodce Quick Start Wizard spustili, během prvního připojení webové konzoly k serveru pro správu. Průvodce Quick Start Wizard můžete také spustit v rozhraní webové konzoly (**Discovery & deployment** → **Deployment & assignment** → **Quick start wizard**). Průvodce Quick Start Wizard může také zkontrolovat, zda jsou nainstalované webové moduly plug-in aktuální, a může stáhnout potřebné aktualizace. Podrobnější informace o průvodci Quick Start Wizard pro webovou konzolu aplikace Kaspersky Security Center najdete v nápovědě k aplikaci Kaspersky Security Center.

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

  Chcete-li nainstalovat webový modul plug-in, vyberte distribuční balíček webového modulu plug-in aplikace Kaspersky Endpoint Security v rozhraní webové konzoly (**Console settings** → **Web 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 konzoly (**Console settings** → **Web plug-ins**). Distribuční balíček webového modulu plug-in lze stáhnout například na webových stránkách společnosti Kaspersky.

Počínaje aplikací Kaspersky Endpoint Security 12.11 pro systém Windows se změnil postup instalace webového modulu plug-in. Distribuční balíček nově obsahuje dva webové moduly plug-in: *Kaspersky Endpoint Security for Windows 14.0.0* a *Unified Protection and Management Plug-in*. Je to důsledek přechodu na jeden jednotný webový modul plug-in pro správu aplikací Kaspersky. Jednotný webový modul plug-in umožňuje vytvořit jednu zásadu pro správu více aplikací Kaspersky (například Kaspersky Endpoint Security pro systém Windows, macOS a Linux). Přechod na sjednocený webový modul plug-in může trvat několik verzí. Po dokončení převodu bude distribuční balíček obsahovat pouze *Unified Protection and Management Plug-in*.

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 konzoly (**Console settings → Web 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 konzoly (**Console settings → Web 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 konzoly (**Console settings → Web 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.

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

- Předchozí verze modulu plug-in administrace produktu Kaspersky Endpoint Security bude odebrána.
- Nová verze modulu plug-in administrace produktu Kaspersky Endpoint Security podporuje správu předchozí verze aplikace Kaspersky Endpoint Security 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.

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

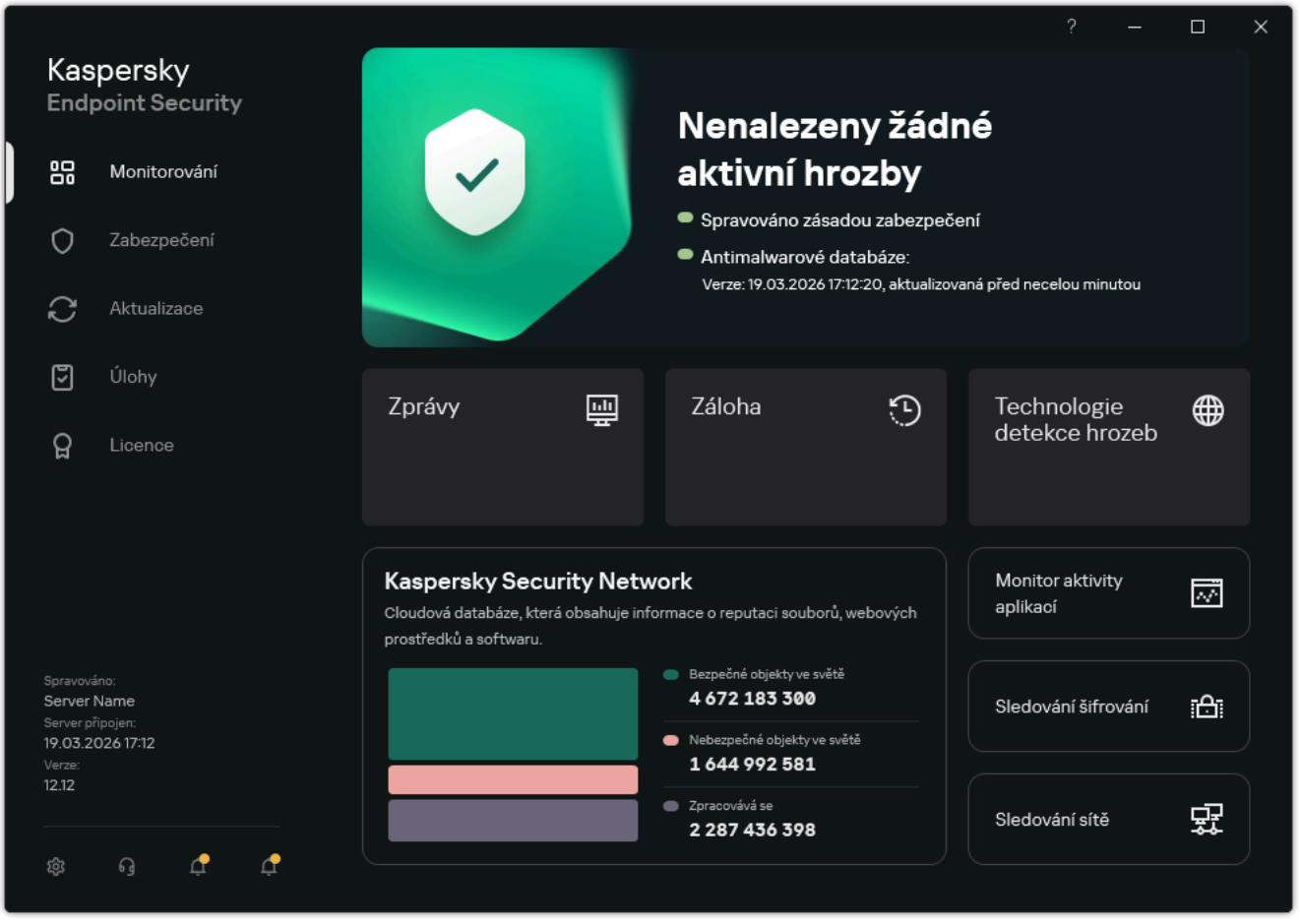
Použití protokolu TLS zajišťuje aplikaci poskytnutím následujících funkcí:

- 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.
- Ověření. 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 Public Key Infrastructure (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, VeriSign, 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 Self-Signed Certificate. 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

Monitorování

- **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 reputaci kontrolovaných webových adres a také informace o reputaci kategorii a reputaci kontrolovaných souborů.
- **Monitor aktivity aplikací**. Zobrazení informací o provozu nainstalovaných aplikací. Monitor aktivity aplikací 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.

Zabezpečení	Provozní stav nainstalovaných součástí. Můžete také přejít ke konfiguraci součástí nebo prohlížení zpráv.
Aktualizace	Můžete spravovat úlohy aktualizace aplikace Kaspersky Endpoint Security. Můžete aktualizovat antivirové databáze a moduly aplikace a vrátit zpět poslední aktualizaci. Správce může skrýt tento oddíl před uživatelem nebo omezit správu úloh.
Úlohy	Můžete spravovat úlohy kontroly aplikace Kaspersky Endpoint Security. Můžete spustit kontrolu malwaru a kontrolu integrity aplikace. Správce může skrýt úlohy před uživatelem nebo omezit správu úloh.
Licence	Správa licence k aplikaci. Můžete si zakoupit licenci, aktivovat aplikaci nebo obnovit předplatné. Můžete také zobrazit informace o aktuální licenci.
	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.

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.

Pokud je ikona aplikace v oznamovací oblasti hlavního panelu skrytá, správce zakázal zobrazování rozhraní aplikace v zásadě.

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, klikněte v místní nabídce aplikace na možnost **Obnovit ochranu**.

  Pozastavení činnosti součástí ochrany a kontroly nemá vliv na výkon úloh aktualizace a kontroly malwaru. 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**. Tímto otevřete 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.

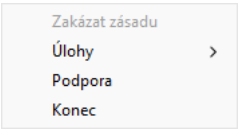


Kontextová nabídka ikony Aplikace

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 aplikací**.
  - **Vrácení databází k předchozí verzi**.
  - **Úplná kontrola**.
  - **Vlastní kontrola**.
  - **Kontrola kritických oblastí**.
  - **Aktualizovat**.
- **Podpora**. Tímto otevřete 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:

- **Zobrazit zjednodušené rozhraní**. 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.
- **Zobrazit uživatelské rozhraní**. 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.

- **Nezobrazovat uživatelské 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Rozhraní**.
4. V bloku **Interakce s uživatelem** proveďte některou z následujících akcí:
   - Zaškrtněte políčko **Zobrazit uživatelské rozhraní**, pokud chcete, aby se v klientském počítači zobrazily následující prvky rozhraní:
     - Složka obsahující název aplikace v nabídce **Spustit**
     - 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 uživatelské rozhraní**, pokud chcete skrýt všechny známky přítomnosti aplikace Kaspersky Endpoint Security v klientském počítači.
5. Pokud chcete zobrazit zjednodušené rozhraní aplikace v klientském počítači s nainstalovanou aplikací Kaspersky Endpoint Security, v bloku **Interakce s uživatelem** zaškrtněte políčko **Zobrazit zjednodušené rozhraní**.

Jak nakonfigurovat místní nastavení aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **User Interaction**.
5. V bloku **Visibility for users** nakonfigurujte způsob zobrazování rozhraní aplikace:
   - **Show the application icon**. Klientský počítač má v oznamovací oblasti ikonu aplikace. V místní nabídce ikony může uživatel provádět operace s aplikací Kaspersky Endpoint Security. Aplikace Kaspersky Endpoint Security také zobrazuje upozornění nad ikonou aplikace.
   - **Do not display application interface for users**. V klientském počítači je hlavní okno aplikace Kaspersky Endpoint Security nepřístupné a je k dispozici pouze ikona v oznamovací oblasti systému. 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.
6. Uložte změny.

Příprava aplikace na používání

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 Quick Start Wizard aplikace Kaspersky Security Center automaticky vytvoří zásadu pro aplikaci Kaspersky Endpoint Security.
- Vytvořte úlohy *Aktualizace databází a modulů aplikace* a *Kontrola malwaru*.

  Úloha *Aktualizace databází a modulů aplikace* je třeba pro zachování aktuálního zabezpečení počítače. Když je provedena tato úloha, aplikace Kaspersky Endpoint Security aktualizuje antivirové databáze a moduly aplikace. Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

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

  Jak vytvořit úlohu Kontrola malwaru v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Kontrola malwaru**.

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 se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, 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.
- **Run only when the computer is idle**. Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.

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 *Kontrola malwaru*. 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 **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. V důsledku toho bude úloha kontroly malwaru provedena v počítačích uživatelů podle určeného plánu.

Jak vytvořit úlohu Kontrola malwaru ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Malware Scan**.
   c. V poli **Task name** zadejte krátký popis, například *Weekly scan*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Chcete-li nakonfigurovat plán úloh, přejděte do vlastností úloh.
   Doporučuje se naplánovat spuštění úlohy alespoň jednou týdně.
8. Zaškrtněte políčko vedle úlohy.
9. Klikněte na tlačítko **Start**.
   Můžete sledovat stav úlohy a počet zařízení, ve kterých byla úloha úspěšně dokončena nebo dokončena s chybou.

V důsledku toho bude úloha kontroly malwaru provedena v počítačích uživatelů podle určeného plánu.

- Optimalizujte výkon aplikace Kaspersky Endpoint Security.

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.

Každé nastavení zásad má atribut („visací zámek"). Stav tohoto atributu určuje, zda bude nastavení předáváno spravovaným zařízením ve skupině pro správu:

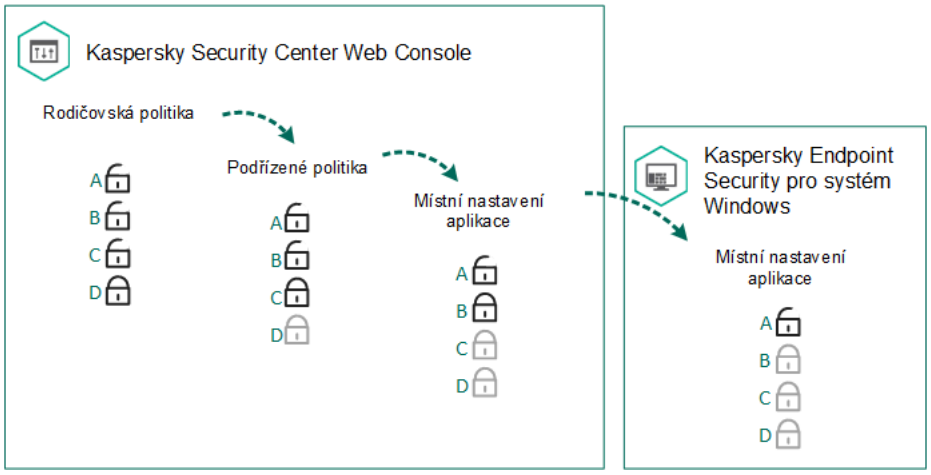
- Pokud je „visací zámek" otevřený ( ), hodnota tohoto nastavení nebude předávána do spravovaných zařízení. Nastavení bude možné změnit v místním rozhraní aplikace. Taková nastavení se označují jako *odemčená*.
- Pokud je „visací zámek" zavřený ( ), bude hodnota tohoto nastavení předávána na spravovaná zařízení a používána na nich. Taková nastavení se označují jako *zamčená*. Blokovaná nastavení není možné měnit v místním rozhraní aplikace.

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.

Dědičnost nastavení

Zásady, jako jsou administrativní skupiny, jsou uspořádány v hierarchii. *Podřízená zásada* je zásada pro vnořené úrovně hierarchie, což je zásada pro vnořené skupiny pro správu a sekundární servery pro správu.

Ve výchozím nastavení podřízená zásada dědí nastavení z nadřazené zásady. Pokud má nastavení v nadřazených zásadách atribut (zavřený „visací zámek"), pak v podřízených zásadách a místním nastavení aplikace bude hodnota tohoto nastavení přepsána v souladu s nadřazenými zásadami a nastavení bude uzamčeno. Dědičnost nastavení z nadřazené zásady můžete v případě potřeby zakázat. 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 přístupová práva k nastavení zásad, v okně vlastností serveru pro správu aplikace Kaspersky Security Center přejděte do části **Security** (ve výchozím nastavení je tato část v rozhraní konzoly skryta).

Revize zásad

Aplikace Kaspersky Security Center sleduje úpravy zásad a vytváří revize. *Revize* je soubor změněných parametrů uložených uživatelem. Revize umožňují porovnat a vrátit změny parametrů zásad. Kromě sady upravených parametrů obsahuje revize informace o uživateli, který změny provedl, a také čas, IP adresu, komentář uživatele a další relevantní údaje.

Chcete-li zobrazit protokol revizí, otevřete vlastnosti zásad a přejděte do části **Revision history**. Podrobnosti o práci s revizemi najdete v nápovědě k aplikaci Kaspersky Security Center.

Vytvoření zásad

Při vytváření zásady průvodce navrhne nastavení, která jsou relevantní pro vybraný režim. Například u režimu Light Agent musíte přidat server pro ochranu (SVM). Při použití aplikace k ochraně serveru SQL musíte přidat předdefinované výjimky z kontroly, aby nebyl narušen provoz serveru. Po výběru režimu průvodce navrhne příslušná nastavení zásad. Tato nastavení pak můžete upravit ve vlastnostech 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 zásadami.

Krok 1. Výběr aplikace pro vytvoření zásady skupiny

Vyberte aplikaci **Kaspersky Endpoint Security for Windows (14.0)**.

Krok 2. Pojmenování zásady skupiny

Zadejte název zásady skupiny, například *Zásady pro kancelář*.

Pomocí průvodce zásadami můžete také vytvořit nové zásady na základě stávajících zásad. Chcete-li tak učinit, při zadávání názvu zásad skupiny zaškrtněte políčko **Use policy settings for an earlier version of the application**. Průvodce také umožňuje vytvořit zásadu aplikace Kaspersky Endpoint Security (KES) na základě zásad jiného řešení, například Kaspersky Security for Windows Server (KSWS) nebo Kaspersky Security for Virtualization Light Agent pro systém Windows.

Krok 3. Účast ve službě Kaspersky Security Network

Přečtěte si a přijměte podmínky Prohlášení o Kaspersky Security Network (KSN).

Krok 4. Výběr režimu používání aplikace v počítačích

V závislosti na zamýšleném použití aplikace Kaspersky Endpoint Security můžete nakonfigurovat zásady pro následující režimy aplikací:

- Standardní režim na ochranu hostitelů

  V tomto režimu můžete vybrat, jak chcete zásady nakonfigurovat:

  - **Vytvořit zásadu s výchozími nastaveními**. Výchozí nastavení jsou považována za optimální. Tato nastavení doporučují odborníci společnosti Kaspersky. Výchozí nastavení poskytují doporučenou úroveň ochrany a optimální využití zdrojů.
  - **Změnit nastavení zásady v průvodci**. Tato metoda umožňuje podrobnou správu nastavení zásad pomocí průvodce. Nastavení zásad můžete také spravovat pomocí konfiguračního souboru aplikace (viz další krok).

- Endpoint Detection and Response Agent na ochranu před pokročilými hrozbami a cílenými útoky.

  Endpoint Detection and Response Agent je aplikace, která se instaluje na jednotlivé pracovní stanice a servery v IT infrastruktuře organizace za účelem podpory řešení Detection and Response od společnosti Kaspersky. V dalším kroku musíte vybrat řešení pro integraci součásti EDR Agent.

- Light Agent na ochranu virtuálních prostředí.

  Chcete-li používat aplikaci v režimu Light Agent, musíte nakonfigurovat připojení k virtuálnímu počítači SVM. Toto nastavení je nutné, aby aplikace fungovala v režimu Light Agent.

Kaspersky Endpoint Security poskytuje společné zásady pro všechny režimy aplikace a typy OS. To znamená, že zásady pokrývají celou sadu nastavení. Aplikace však může ignorovat některá nastavení zásad, protože aplikace Kaspersky Endpoint Security je nasazena v režimu, ve kterém nejsou některé funkce k dispozici. Například při používání aplikace v režimu Endpoint Detection and Response Agent jsou k dispozici pouze nastavení, která jsou relevantní pro integraci s řešeními Kaspersky Detection and Response a pro integraci s KUMA.

Pro různé režimy a typy operačního systému doporučujeme používat různé zásady.

Krok 5. Import nastavení

Tento krok je k dispozici, pokud v kroku 4 vyberete ruční konfiguraci zásad.

Zásady můžete vytvořit na základě nastavení aplikace Kaspersky Endpoint Security z konfiguračního souboru CFG. Při importu konfiguračního souboru aplikace nemusí mít průvodce k dispozici všechna nastavení zásad. V nastavení aplikace chybí například profily zásad. Pokud chcete do zásad přenést všechna nastavení a profily, můžete importovat jinou zásadu ze souboru KLP.

Při importu konfiguračního souboru aplikace Kaspersky Endpoint Security nepřenáší hesla ke kryptokontejnerům. Pokud při připojování k serverům používáte obousměrné ověřování, musíte úplně zadávat hesla ke kryptokontejnerům ručně.

Krok 6–10. Konfigurace nastavení zásad

Tento krok je k dispozici, pokud v kroku 4 vyberete ruční konfiguraci zásad.

Postupujte podle pokynů pro správu nastavení zásad.

Krok 11. Konfigurace důvěryhodné zóny

Nakonfigurujte důvěryhodnou zónu. Můžete přidat předdefinované výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou také pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security v režimu Light Agent ve virtuálních prostředích Citrix a VMware.

Krok 12. Výběr stavu zásady

- **Active**. Po další synchronizaci bude zásada v počítači použita jako aktivní zásada.

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.

- **Inactive**. Slouží jako záložní zásada. V případě potřeby lze neaktivní zásadu přepnout do aktivního stavu.

  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.

- **Out-of-office**. Zásada je aktivována v případě, že počítač opustí hranice sítě organizace.

Ukončete průvodce.

Jak vytvořit zásadu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na tlačítko **Add**.

   Spustí se průvodce zásad.
3. Vyberte aplikaci Kaspersky Endpoint Security a klikněte na tlačítko **Next**.
4. Přečtěte si a přijměte podmínky Prohlášení o Kaspersky Security Network (KSN) a klikněte na tlačítko **Next**.
5. Vyberte režim aplikace:

   - Standard mode to protect workstations and servers
   - Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

     Pokud vyberete tento režim, můžete vytvořit zásady pro integraci počítače s řešeními aplikace Kaspersky Detection and Response. Průvodce vás vyzve, abyste nakonfigurovali integraci pro řešení Kaspersky Managed Detection and Response a poté pro Kaspersky Anti Targeted Attack Platform (EDR).
   - Light Agent to protect virtual environments.

     Pokud vyberete tento režim, musíte v dalším kroku nakonfigurovat připojení k serveru pro ochranu (SVM). Toto nastavení je nutné, aby aplikace fungovala v režimu Light Agent.

   Kaspersky Endpoint Security poskytuje společné zásady pro všechny režimy aplikace a typy OS. To znamená, že zásady pokrývají celou sadu nastavení. Aplikace však může ignorovat některá nastavení zásad, protože aplikace Kaspersky Endpoint Security je nasazena v režimu, ve kterém nejsou některé funkce k dispozici. Například při používání aplikace v režimu Endpoint Detection and Response Agent jsou k dispozici pouze nastavení, která jsou relevantní pro integraci s řešeními Kaspersky Detection and Response a pro integraci s KUMA.

   > Pro různé režimy a typy operačního systému doporučujeme používat různé zásady.

6. Nakonfigurujte důvěryhodnou zónu. Můžete přidat předdefinované výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou také pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security v režimu Light Agent ve virtuálních prostředích Citrix a VMware.
7. Na kartě **General** můžete provést následující akce:

   - Změňte název zásady.
   - Vyberte stav zásady:

     - **Active**. Po další synchronizaci bude zásada v počítači použita jako aktivní zásada.

       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.
     - **Inactive**. Slouží jako záložní zásada. V případě potřeby lze neaktivní zásadu přepnout do aktivního stavu.

       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.
     - **Out-of-office**. Zásada je aktivována v případě, že počítač opustí hranice sítě organizace.
   - Nakonfigurujte dědění nastavení:

- **Inherit settings from parent policy**. 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.
- **Force inheritance of settings in child policies**. Pokud je přepínací tlačítko v zapnutém stavu, hodnoty nastavení zásad jsou rozšířeny do podřízených zásad. Ve vlastnostech podřízených zásad se přepínací tlačítko **Inherit settings from parent policy** 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.

8. Na kartě **Application settings** můžete nakonfigurovat nastavení zásad aplikace Kaspersky Endpoint Security.
9. Ukončete průvodce.

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 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 nápovědě k aplikaci Kaspersky Security Center.

Export a import zásady

Aplikace Kaspersky Endpoint Security umožňuje exportovat zásadu s nastavením a profily do souboru KLP. Funkci exportu/importu zásad pak můžete použít k zálohování zásad, migraci zásad na jiný server nebo například k migraci zásad z aplikace Kaspersky Security Center Windows do Kaspersky Security Center Linux. Podrobnosti o správě zásad najdete v nápovědě k aplikaci Kaspersky Security Center.

Jak exportovat a importovat zásadu 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. Postup exportu zásady:
   a. Klikněte na zásadu, kterou chcete exportovat.
   b. V pravé části okna klikněte na odkaz **Export policy to file**.
   c. V okně, které se otevře, zadejte název souboru KLP, do kterého chcete zásadu exportovat, a vyberte složku, do které chcete tento soubor uložit.
   d. Uložte soubor.
5. Postup importu zásad:
   a. Klikněte na tlačítko **Import policy from file**.
   b. V okně, které se otevře, vyberte soubor KLP zásady, který chcete importovat.
   c. Otevřete soubor.

Tímto způsobem přidáte novou zásadu se stavem *Inactive policy*.

Jak exportovat a importovat zásadu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Postup exportu zásady:
   a. Zaškrtněte políčka vedle zásady, kterou chcete upravit.
   b. Klikněte na tlačítko **Export**.
   c. V okně, které se otevře, zadejte název souboru KLP, do kterého chcete zásadu exportovat, a vyberte složku, do které chcete tento soubor uložit.
   d. Uložte soubor.
3. Postup importu zásad:

a. Klikněte na tlačítko **Import**.

b. Vyberte soubor zásad KLP, který chcete importovat.

c. Po úspěšném zpracování zásad vyberte skupinu pro správu, na kterou chcete zásady použít.

d. Kliknutím na tlačítko **Complete** dokončete import zásady.

Tímto způsobem přidáte novou zásadu se stavem *Inactive*.

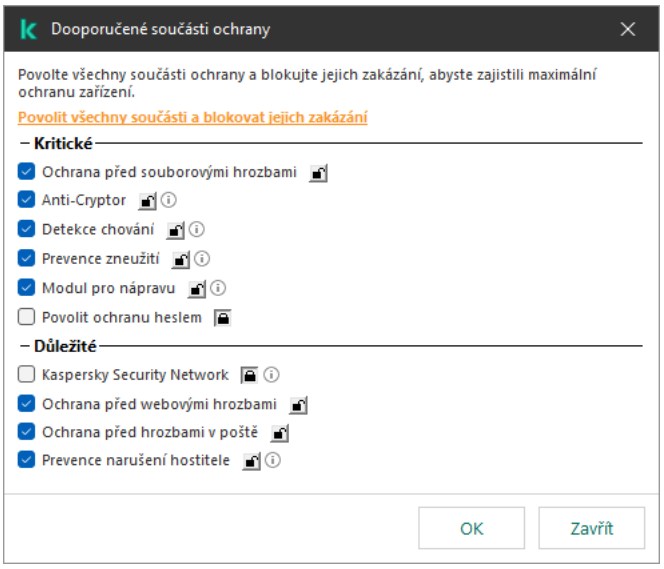
Ukazatel úrovně zabezpečení

Ukazatel úrovně zabezpečení se zobrazí v horní části okna vlastností 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.
    - Ochrana služeb aplikace před externí správou.
  - **Důležité**. Tato kategorie obsahuje následující součásti:
    - Kaspersky Security Network.
    - Ochrana před webovými hrozbami.
    - Ochrana před hrozbami v poště.
    - Prevence narušení hostitele.
    - Ochrana heslem.
- **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 **Dooporučené součásti ochrany**. V tomto okně můžete povolit libovolné doporučené součásti ochrany.

Po upgradu aplikace může indikátor úrovně ochrany ukazovat nižší úroveň ochrany než před upgradem. Důvodem je, že novější verze aplikace zavádějí nové součásti nebo funkce, které jsou důležité pro zabezpečení počítače. Po upgradu aplikace musíte spravovat nové nastavení a zajistit, aby úroveň ochrany zůstala vysoká.



Indikátor úrovně zabezpečení zásad

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:

- **Kontrola malwaru**. Aplikace Kaspersky Endpoint Security zkontroluje, zda se v oblastech počítače určených v nastavení úlohy nenacházejí viry či jiné hrozby. Úloha *Kontrola malwaru* je vyžadována pro fungování aplikace Kaspersky Endpoint Security a je vytvořena v průběhu průvodce Quick Start Wizard. Doporučuje se naplánovat spuštění úlohy alespoň jednou týdně.
- **Přidání klíče**. 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.
- **Změna součástí 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 databází a modulů aplikace**. Aplikace Kaspersky Endpoint Security aktualizuje databáze a moduly aplikace. Úloha *Aktualizace databází a modulů aplikace* je vyžadována pro fungování aplikace Kaspersky Endpoint Security a je vytvořena v průběhu průvodce Quick Start Wizard. Doporučuje se nakonfigurovat plán, který spustí úlohu alespoň jednou denně.
- **Výmaz dat**. 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 aplikací**. 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.

Pokud aplikace funguje jako součást řešení Endpoint Detection and Response od společnosti Kaspersky, můžete spouštět další úlohy jako akce reakce na detekci (responses). Procesy můžete například vzdáleně ukončit pomocí úlohy *Ukončit proces*.

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

Vytváření 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 **New task**.
   Spustí se průvodce úlohou.
4. Postupujte podle pokynů průvodce úloh.

Jak vytvořit úlohu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte úlohu, kterou chcete spustit v počítačích uživatelů.
   c. Do pole **Task name** zadejte krátký popis.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete 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 (**Monitoring** → **Event selections**). Další informace o výběru události najdete v nápovědě k aplikaci Kaspersky Security Center. Výsledky spuštění úlohy se uloží také místně v protokolu událostí systému Windows a ve zprávách aplikace Kaspersky Endpoint Security.

Správa přístupu k úlohám

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Místní úlohy** → **Správa úloh**.
4. Nakonfigurujte režim správy úloh (viz tabulka níže).

5. Uložte změny.

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

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **User Interaction**.
5. V části **Permitted actions** nakonfigurujte režim správy úloh (viz tabulka níže).
6. Uložte změny.

Nastavení správy úloh

Parametr	Popis
Access to local tasks	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 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.
View group tasks	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.
Manage group tasks	Pokud je políčko zaškrtnuté, uživatelé mohou spouštět a zastavovat úlohy skupiny uvedené v konzole aplikace 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 konzole aplikace 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 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 (14.0)** a dvojitým kliknutím otevřete vlastnosti aplikace.
7. V části **Obecná nastavení** nakonfigurujte aplikaci Kaspersky Endpoint Security a také zprávy a úložiště.
   Zbývající části okna vlastností aplikace jsou standardní pro aplikaci 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.

8. Uložte změny.

Jak nakonfigurovat místní nastavení aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. Nakonfigurujte místní nastavení aplikace.
7. Uložte změny.

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)

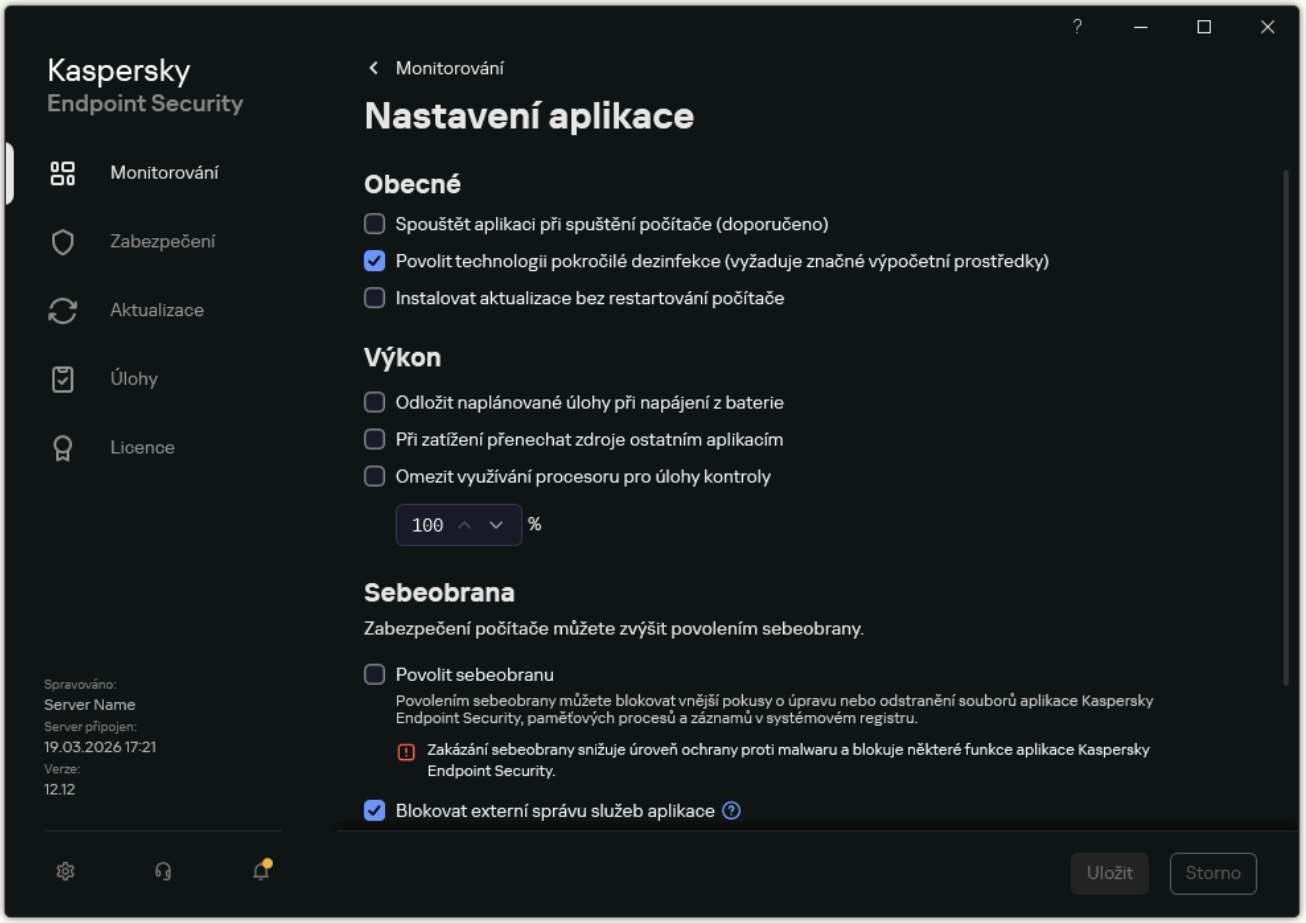
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. Pomocí zaškrtávacího políčka **Spouštět aplikaci při spuštění počítače (doporučeno)** nakonfigurujte spouštění aplikace.
5. Uložte změny.

Jak nakonfigurovat spouštění aplikace Kaspersky Endpoint Security ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **User Interaction**.
5. Pomocí zaškrtávacího políčka **Start Kaspersky Endpoint Security on computer startup (recommended)** nakonfigurujte spouštění aplikace.
6. Uložte změny.

Jak nakonfigurovat spuštění aplikace Kaspersky Endpoint Security v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. Pomocí zaškrtávacího políčka **Spouštět aplikaci při spuštění počítače (doporučeno)** nakonfigurujte spouštění aplikace.
4. Uložte změny.

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 **Protection status**.

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 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 (14.0)** a dvojitým kliknutím otevřete vlastnosti aplikace.
7. Proveďte jednu z následujících akcí:

- 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 konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Klikněte na název počítače, ve kterém chcete spustit nebo zastavit aplikaci Kaspersky Endpoint Security.
   Otevře se okno vlastností počítače.
3. Vyberte kartu **Applications**.
4. Zaškrtněte políčko naproti možnosti **Kaspersky Endpoint Security pro systém Windows**.
5. Klikněte na tlačítko **Spustit** nebo **Zastavit**.

[Jak spustit nebo zastavit aplikaci Kaspersky Endpoint Security z příkazového řádku]

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, kde je umístěn spustitelný soubor klpsm.exe.
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`.

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



Spuštění a zastavení aplikace z příkazového řádku

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.

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.
- Provádět vzdálenou instalaci aplikace Kaspersky Endpoint Security prostřednictvím aplikace Kaspersky Security Center s předdefinovanými nastaveními.
- Přenést nastavení aplikace do zásad.
- Přenášet nastavení aplikace Kaspersky Endpoint Security z jednoho počítače do druhého (viz pokyny níže).

Export konfiguračního souboru

Postup vytvoření konfiguračního souboru:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → 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. V případě potřeby zadejte heslo pro export konfigurace aplikace do souboru.

   Chcete-li uložit konfigurační soubor, musí být povolena Ochrana heslem. Uživatel musí mít oprávnění **Export nastavení**.

6. Uložte soubor.

Aplikace tak vytvoří konfigurační soubor. Konfigurační soubor může obsahovat podrobnosti o uživatelském účtu, proto Kaspersky Endpoint Security soubor šifruje. Konfigurační soubor nelze upravovat. Při jakémkoli pokusu o úpravu konfiguračního souboru dojde k jeho poškození.

Import konfiguračního souboru

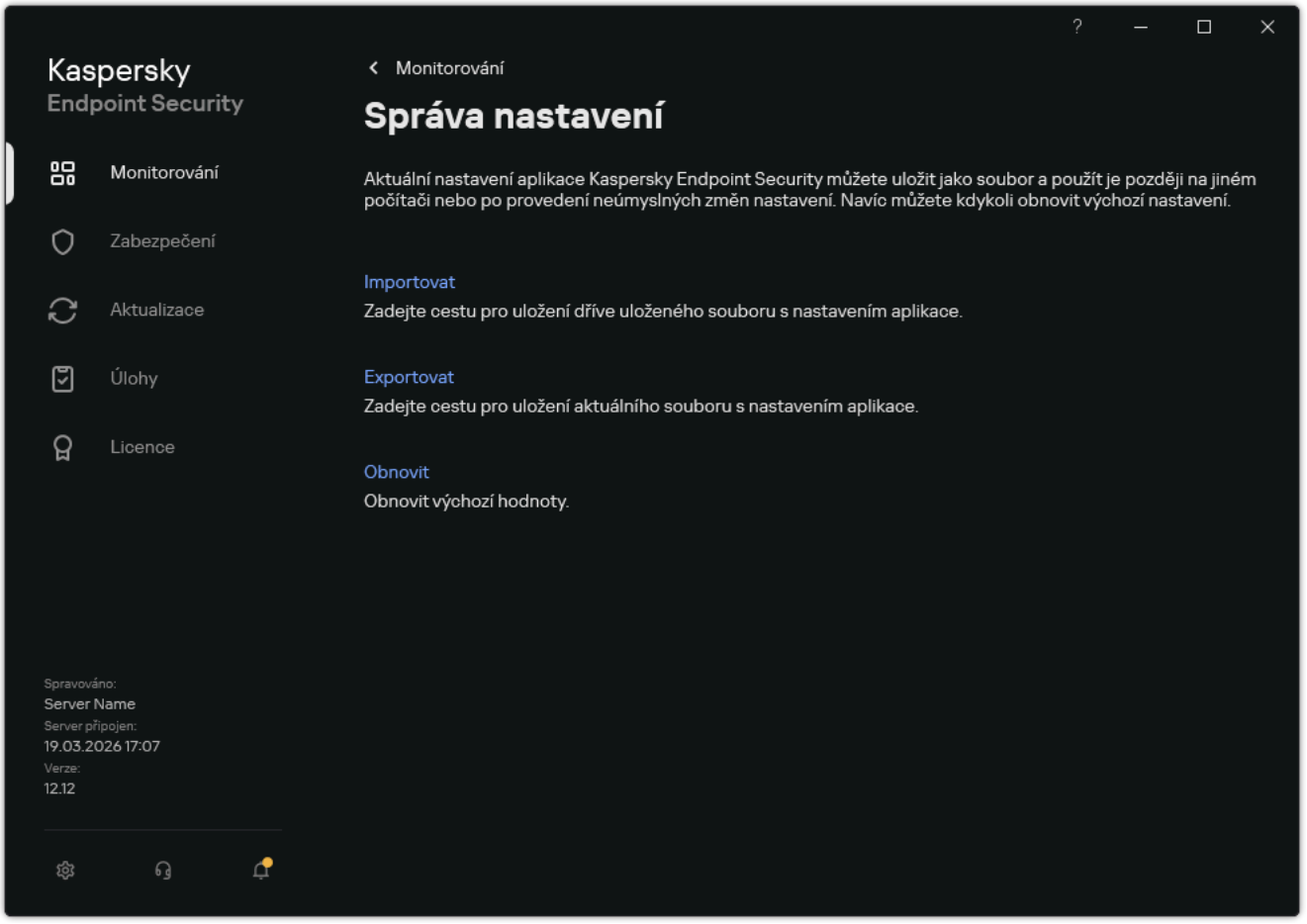
Konfigurační soubor může obsahovat podrobnosti o uživatelských účtech přidaných do aplikace. Pokud soubor importujete do stejného počítače, kde byl soubor vytvořen, Kaspersky Endpoint Security importuje hesla uživatelských účtů. Pokud soubor importujete do jiného počítače, musíte zadat hesla ručně.

Při importu konfiguračního souboru aplikace Kaspersky Endpoint Security nepřenáší hesla ke kryptokontejnerům. Pokud při připojování k serverům používáte obousměrné ověřování, musíte úplně zadávat hesla ke kryptokontejnerům ručně.

Postup importu nastavení aplikace Kaspersky Endpoint Security z konfiguračního souboru:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Správa nastavení**.
3. Klikněte na tlačítko **Importovat**.
4. V okně, které se otevře, zadejte cestu ke konfiguračnímu souboru.
5. Otevřete soubor.

Všechny hodnoty nastavení aplikace Kaspersky Endpoint Security budou určeny podle vybraného konfiguračního souboru.



Správa nastavení zásad

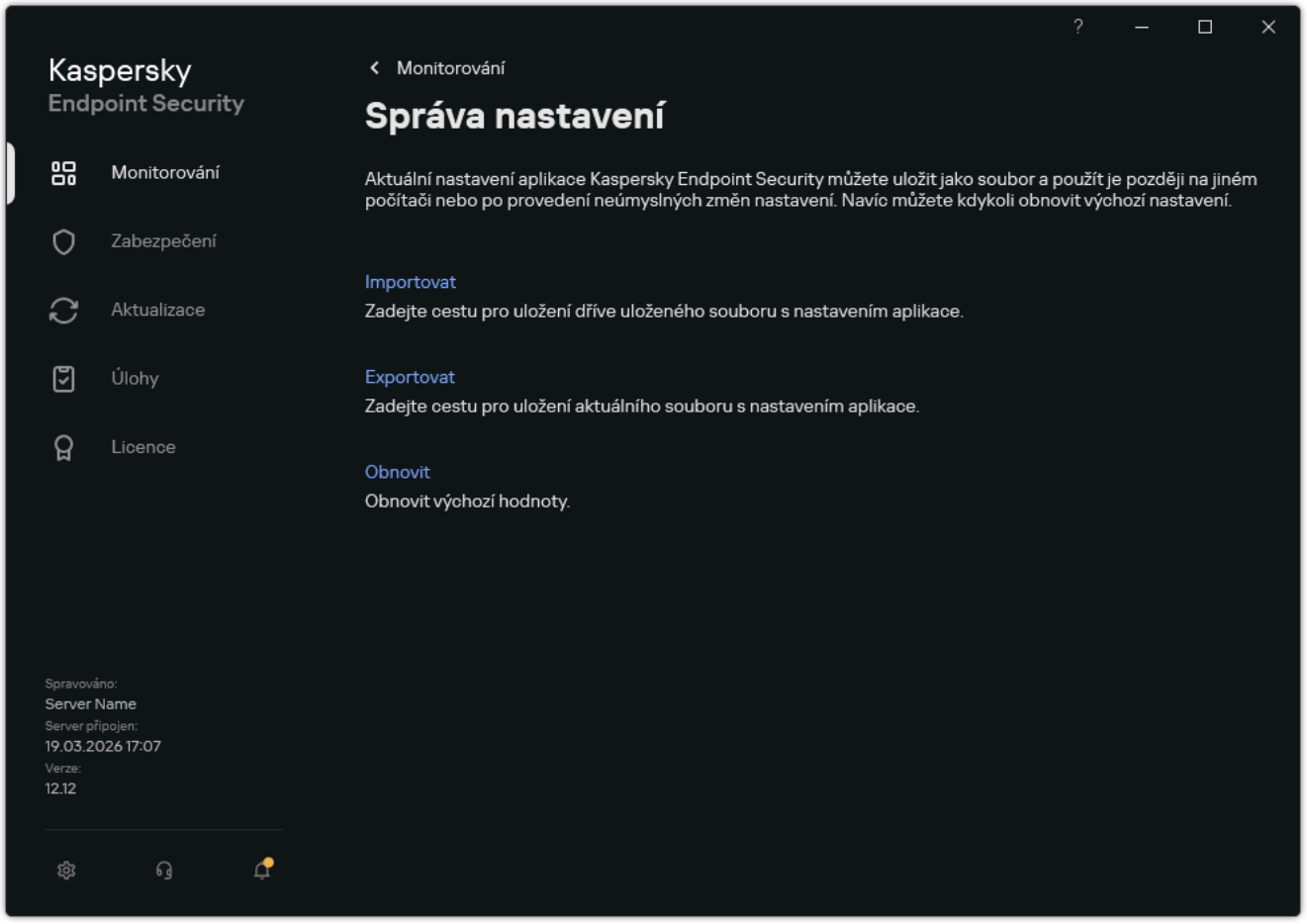
Obnovení výchozího nastavení aplikace

Kdykoli můžete obnovit nastavení aplikace doporučené společností Kaspersky. Po obnovení nastavení bude pro všechny součásti ochrany nastavena **Doporučená** úroveň zabezpečení.

Postup obnovení výchozího nastavení aplikace:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Správa nastavení**.
3. Klikněte na tlačítko **Obnovit**.

4. Uložte změny.



Správa nastavení zásad

Výkon aplikace Kaspersky Endpoint Security a kompatibilita s jinými aplikacemi

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

Spotřeba prostředků počítače při kontrole počítače může zvýšit zatížení subsystémů procesoru a pevného disku. Aby nedocházelo k problémům se souběžnými operacemi při zvýšeném zatížení procesoru a pevného disku, dokáže aplikace Kaspersky Endpoint Security uvolnit prostředky pro jiné aplikace.

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.

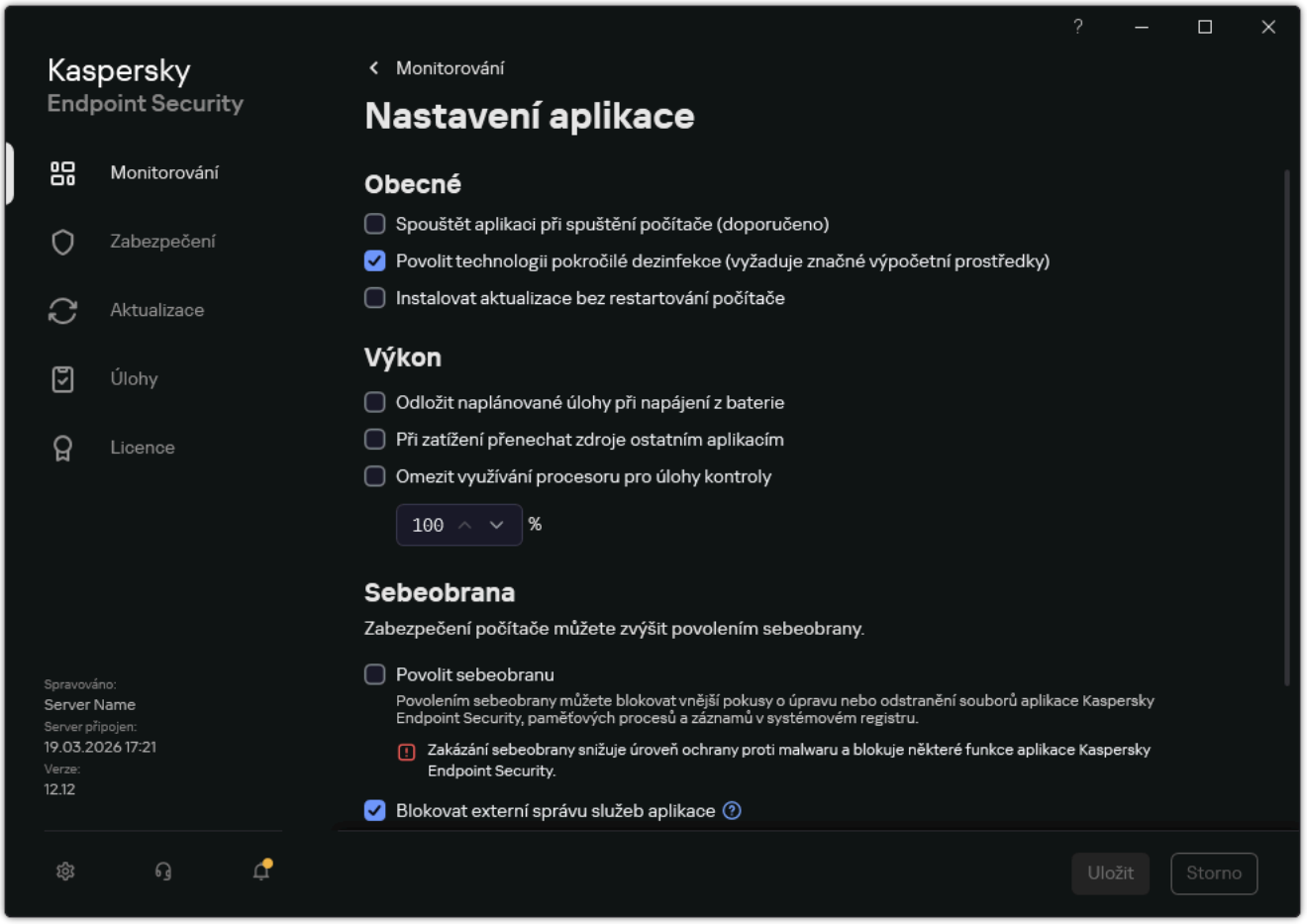
V počítačích se systémy Microsoft Windows pro servery není zobrazení žádosti o restartování možné kvůli vlastnostem aplikace Kaspersky Endpoint Security. Neplánované restartování souborového serveru může vést k problémům, jako je dočasná nedostupnost dat na serveru či ztráta neuložených dat. Souborové 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 pokročilá dezinfekce. Pokud chcete odstranit aktivní infekci serveru, povolte technologii aktivní dezinfekce a spusťte skupinovou úlohu *Kontrola malwaru* v době, která je vhodná pro uživatele serveru.

Povolení nebo zakázání režimu úspory energie

Postup povolení nebo zakázání režimu úspory energie:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. V bloku **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:

- *Aktualizace databází a modulů aplikace*
- *Úplná kontrola*
- *Kontrola kritických oblastí*
- *Vlastní kontrola*
- *Kontrola integrity aplikací*
- *Kontrola IOC*.

4. Uložte změny.

Povolení nebo zakázání uvolnění prostředků pro jiné aplikace

Spotřeba prostředků počítače aplikací Kaspersky Endpoint Security při kontrole počítače může zvýšit zatížení subsystémů procesoru a pevného disku. To může zpomalovat jiné aplikace. Pro optimalizaci výkonu poskytuje aplikace Kaspersky Endpoint Security *režim pro přenos prostředků do jiných aplikací*. V tomto režimu může operační systém v případě vysokého zatížení procesoru snížit prioritu vláken úloh kontroly aplikace Kaspersky Endpoint Security. To umožňuje přerozdělit prostředky operačního systému jiným aplikacím. Úlohy kontroly tak získají méně času procesoru. Aplikace Kaspersky Endpoint Security proto bude kontrolovat počítač déle. Aplikace ve výchozím nastavení uvolňuje prostředky pro jiné aplikace.

Jak povolit nebo zakázat přenechání zdrojů ostatním aplikacím při zatížení v konzole pro správu (MMC)

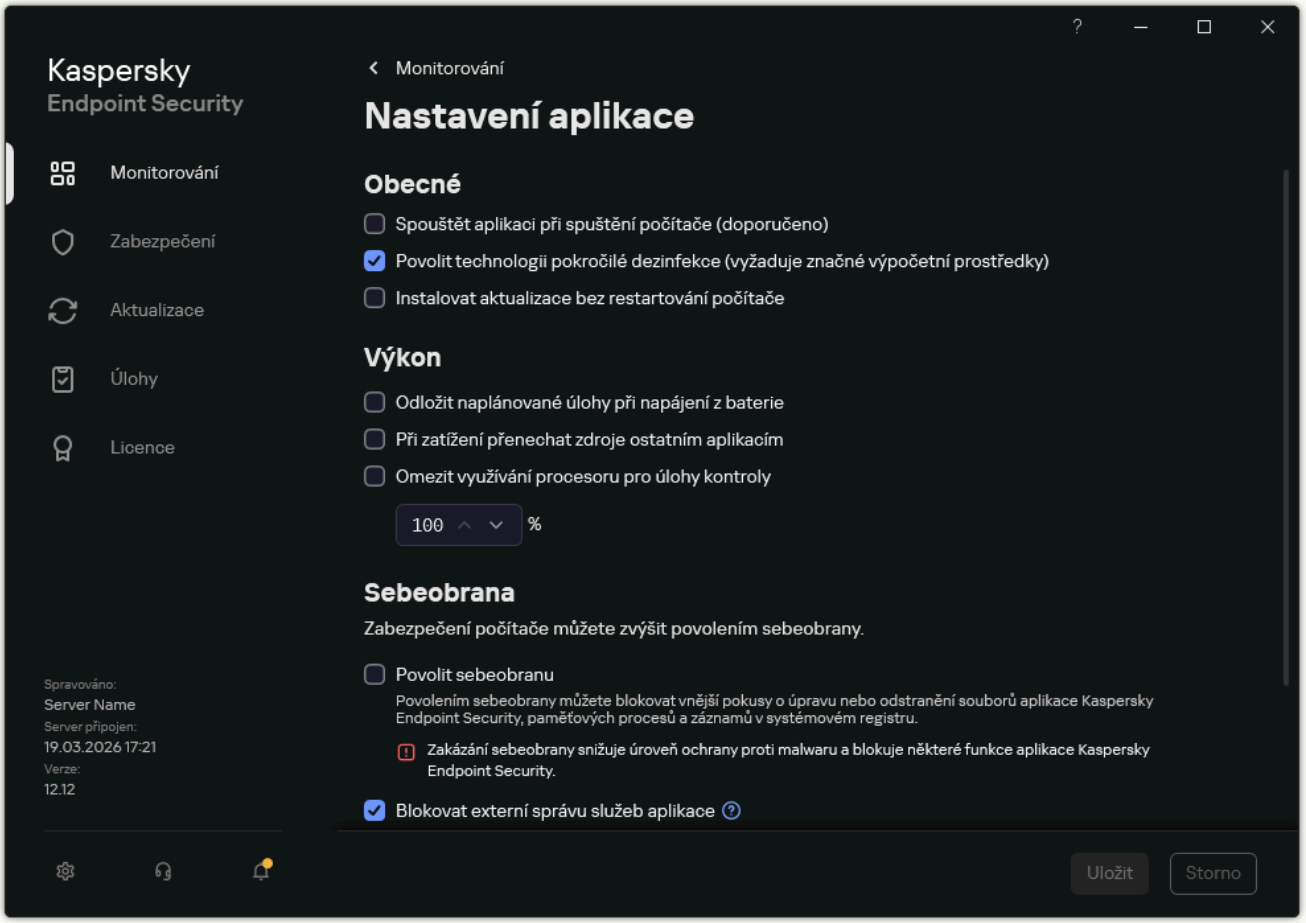
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V bloku **Výkon** pomocí zaškrtávacího políčka **Při zatížení přenechat zdroje ostatním aplikacím** povolíte nebo zakážete přenechávání prostředků jiným aplikacím.
5. Uložte změny.

Jak povolit nebo zakázat přenechání zdrojů ostatním aplikacím při zatížení ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Performance**.
5. V bloku **Concede resources to other applications** přepínačem **Concede resources to other applications** povolíte nebo zakážete přenechávání prostředků jiným aplikacím.
6. Uložte změny.

Jak povolit nebo zakázat přenechání zdrojů ostatním aplikacím při zatížení v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. V bloku **Výkon** pomocí zaškrtávacího políčka **Při zatížení přenechat zdroje ostatním aplikacím** povolíte nebo zakážete přenechávání prostředků jiným aplikacím.

4. Uložte změny.

Doporučené postupy pro optimalizaci výkonu aplikace Kaspersky Endpoint Security

Při nasazování aplikace Kaspersky Endpoint Security pro Windows můžete ke konfiguraci ochrany počítače a optimalizaci výkonu použít následující doporučení. Další informace o řešení problémů s výkonem počítače naleznete ve znalostní bázi technické podpory.

Obecné

Nakonfigurujte obecná nastavení aplikace v souladu s následujícími doporučeními:

1. Upgradujte Kaspersky Endpoint Security na nejnovější verzi.

   Novější verze aplikace mají opravené chyby, vylepšenou stabilitu a optimalizovaný výkon.

2. Povolte součásti ochrany s výchozím nastavením.

   Výchozí nastavení jsou považována za optimální. Tato nastavení doporučují odborníci společnosti Kaspersky. Výchozí nastavení poskytují doporučenou úroveň ochrany a optimální využití zdrojů. V případě potřeby můžete obnovit výchozí nastavení aplikace.

3. Povolte funkce optimalizace výkonu aplikace.

   Aplikace má funkce optimalizace výkonu: režim úspory energie a přenechání zdrojů jiným aplikacím. Ujistěte se, že jsou tyto možnosti povoleny.

Kontrola malwaru na pracovních stanicích

U kontroly malwaru pracovních stanic doporučujeme povolit úlohu 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. Nastavení kontroly na pozadí jsou považována za optimální. Tato nastavení doporučují odborníci společnosti Kaspersky. Pro provedení kontroly malwaru počítače tedy můžete použít pouze režim kontroly na pozadí bez použití dalších úloh kontroly.

Pokud kontrola na pozadí nevyhovuje vašim potřebám, nakonfigurujte úlohu *Kontrola malwaru* úkol v souladu s následujícími doporučeními:

1. Nastavte limit spotřeby prostředků CPU při kontrole počítače.

Můžete omezit využití CPU při provádění úlohy *Kontrola malwaru*. Chcete-li to provést, v nastavení aplikace zadejte maximální procento zatížení CPU pro všechna jádra, která lze využít při kontrole počítače. To může prodloužit dobu potřebnou ke kontrole počítače.

2. Nakonfigurujte optimální plán kontrol počítače.

   Úlohu můžete nakonfigurovat, aby se spouštěla, když počítač pracuje s minimální zátěží. Můžete například nakonfigurovat, aby se úloha spouštěla v noci nebo o víkendech.

   Pokud uživatelé vypnou počítač mimo pracovní dobu, můžete povolit funkci Wake-on-LAN. Funkce Wake-on-LAN umožňuje vzdálené napájení počítače odesláním speciálního signálu po místní síti. Chcete-li tuto funkci používat, musíte v nastavení systému BIOS povolit Wake-on-LAN. Můžete také nechat počítač automaticky vypnout po dokončení kontroly.

   Pokud se vám nepodařilo nakonfigurovat optimální plán kontroly, nastavte úlohy tak, aby se spouštěly pouze při nečinnosti počítače. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena.

3. Definujte rozsah kontroly.

   Vyberte následující objekty pro kontrolu (minimální sada rozsahů kontroly):

   - Paměť jádra
   - Běžící procesy a Spouštěcí objekty
   - Spouštěcí sektory
   - %systemroot% (bez podsložek)
   - %systemroot%\System (bez podsložek)
   - %systemroot%\System32 (bez podsložek)
   - %systemroot%\System32\drivers (bez podsložek)
   - %systemroot%\SysWOW64 (bez podsložek)
   - %systemroot%\SysWOW64\drivers (bez podsložek)

4. Zapněte technologie iSwift a iChecker.

   - 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).

   Technologie iSwift a iChecker můžete zapnout pouze v rozhraní konzoly pro správu (MMC) a Kaspersky Endpoint Security. Tyto technologie nelze zapnout ve webové konzole v aplikaci Kaspersky Security Center.

5. Zakázat kontrolu archivů chráněných heslem.

   Pokud je povolena kontrola archivů chráněných heslem, zobrazí se před kontrolou archivu výzva k zadání hesla. Protože se doporučuje naplánovat úlohu mimo pracovní dobu, uživatel nemůže zadat heslo. Můžete ručně kontrolovat archivy chráněné heslem.

6. Zakázat současné spuštění více úloh kontroly.

   Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače.

Kontrola malwaru na serverech

Nakonfigurujte úlohu *Kontrola malwaru* v souladu s následujícími doporučeními:

1. Nastavte limit spotřeby prostředků CPU při kontrole počítače.

   Můžete omezit využití CPU při provádění úlohy *Kontrola malwaru*. Chcete-li to provést, v nastavení aplikace zadejte maximální procento zatížení CPU pro všechna jádra, která lze využít při kontrole počítače. To může prodloužit dobu potřebnou ke kontrole počítače.

2. Nakonfigurujte optimální plán kontrol počítače.

   Úlohu můžete nakonfigurovat, aby se spouštěla, když počítač pracuje s minimální zátěží. Můžete například nakonfigurovat, aby se úloha spouštěla v noci nebo o víkendech.

3. Zapněte technologie iSwift a iChecker.

   - 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).

   Technologie iSwift a iChecker můžete zapnout pouze v rozhraní konzoly pro správu (MMC) a Kaspersky Endpoint Security. Tyto technologie nelze zapnout ve webové konzole v aplikaci Kaspersky Security Center.

4. Zakázat kontrolu archivů chráněných heslem.

   Pokud je povolena kontrola archivů chráněných heslem, zobrazí se před kontrolou archivu výzva k zadání hesla. Protože se doporučuje naplánovat úlohu mimo pracovní dobu, uživatel nemůže zadat heslo. Můžete ručně kontrolovat archivy chráněné heslem.

5. Zakázat současné spuštění více úloh kontroly.

   Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače.

Kaspersky Security Network

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 reputaci kontrolovaných webových adres a také informace o reputaci kategorii a reputaci kontrolovaných souborů.

Upravte nastavení služby Kaspersky Security Network v souladu s následujícími doporučeními:

1. Povolte rozšířený režim KSN.

   Rozšířený režim služby KSN je režim, ve kterém aplikace Kaspersky Endpoint Security odesílá společnosti Kaspersky více údajů.

2. Konfigurace služby Kaspersky Private Security Network.

   Kaspersky Private Security Network (KPSN) 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.

3. Povolit režim cloudu.

   Režim cloudu 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.

Kontrola malwaru

Kontrola malwaru je zásadní pro bezpečnost počítače. Pravidelně provádějte kontrolu malwaru, 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;
- záloha 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 používat 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:

- systémová paměť;
- objekty načítané při spouštění operačního systému;
- záloha operačního systému;
- 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 aplikací

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

Kontrola počítače

Kontrola je zásadní pro bezpečnost počítače. Pravidelně provádějte kontrolu malwaru, abyste zabránili šíření malwaru, který nebyl zjištěn součástmi ochrany z důvodu nízkého nastavení úrovně zabezpečení nebo z jiných důvodů. Tato součást poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Kaspersky Endpoint Security má předdefinované následující standardní úlohy: *Úplná kontrola*, *Kontrola kritických oblastí*, *Vlastní kontrola*. Pokud má vaše organizace nasazen administrativní systém Kaspersky Security Center, můžete vytvořit úlohu *Kontrola malwaru* a nakonfigurovat kontrolu.

Jak spustit úlohu kontroly malwaru v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Vyberte úlohu kontroly a dvojitým kliknutím otevřete vlastnosti této úlohy.
   V případě potřeby vytvořte úlohu *Kontrola malwaru*.
4. V okně vlastností úlohy vyberte část **Nastavení**.

5. Nakonfigurujte úlohu kontroly (viz tabulka níže).

   Pokud je třeba, nakonfigurujte plán úloh kontroly.

6. Uložte změny.

7. Spusťte úlohu kontroly.

Aplikace Kaspersky Endpoint Security spustí kontrolu počítače. Pokud uživatel přerušil provádění úlohy, například vypnutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla kontrola přerušena.

Jak spustit úlohu kontroly malwaru ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu kontroly.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Application settings**.

4. Nakonfigurujte úlohu kontroly (viz tabulka níže).

   Pokud je třeba, nakonfigurujte plán úloh kontroly.

5. Uložte změny.

6. Spusťte úlohu kontroly.

Aplikace Kaspersky Endpoint Security spustí kontrolu počítače. Pokud uživatel přerušil provádění úlohy, například vypnutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla kontrola přerušena.

Jak spustit úlohu kontroly v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.

2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.

3. Nakonfigurujte úlohu kontroly (viz tabulka níže).

   Pokud je třeba, nakonfigurujte plán úloh kontroly.

4. Uložte změny.

5. Spusťte úlohu kontroly.

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**. Pokud se úloha kontroly nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

Chcete-li optimalizovat výkon aplikace Kaspersky Endpoint Security během kontroly počítače, můžete spravovat rozšířená nastavení úlohy *Úplná kontrola* a omezit využití prostředků procesoru.

V aplikaci Kaspersky Security Center můžete také úlohu *Kontrola na pozadí* místo úlohy *Úplná kontrola* a optimalizovat tak výkon aplikace. Neovlivní to úroveň zabezpečení počítače. Kontrolu na pozadí nelze konfigurovat.

Výsledkem je, že aplikace Kaspersky Endpoint Security zkontroluje počítač, a pokud je zjištěna hrozba, provede akci nakonfigurovanou v nastavení aplikace. Aplikace se obvykle pokusí dezinfikovat infikované soubory. Infikované soubory tak mohou získat následující stavy:

- **Odloženo**. Infikovaný soubor nelze dezinfikovat. Aplikace infikovaný soubor odstraní po restartu počítače.
- **Zaprotokolováno**. Infikovaný soubor nelze dezinfikovat. Aplikace přidává informace o zjištěných infikovaných souborech do seznamu aktivních hrozeb.
- **Zápis není podporován** nebo **Chyba zápisu**. Infikovaný soubor nelze dezinfikovat. Aplikace nemá přístup pro zápis.
- **Již zpracováno**. Aplikace v minulosti zjistila infikovaný soubor. Aplikace infikovaný soubor dezinfikuje nebo odstraní po restartu počítače.

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 aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Hloubková kontrola**.
- **Doporučená**. Aplikace Kaspersky Endpoint Security kontroluje všechny typy souborů. Při kontrole složených souborů aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Střední kontrola**.
- **Nízká**. Kaspersky Endpoint Security kontroluje pouze zadané formáty souborů. Při kontrole složených souborů aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Lehká kontrola**.

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.

Akce při zjištění hrozby

Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, 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 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.

Spustit pokročilou dezinfekci okamžitě

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

Pokročilá dezinfekce během úlohy antivirové kontroly v počítači je provedena, pouze pokud je ve vlastnostech zásad použitých na tento počítač povolena funkce Pokročilá dezinfekce.

Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security dezinfikuje aktivní infekci ihned poté, co byla detekována během provádění úlohy antivirové kontroly. Po dezinfekci aktivní infekce Kaspersky Endpoint Security restartuje počítač bez vyzvání uživatele.

Pokud toto políčko není zaškrtnuto, aplikace Kaspersky Endpoint Security nedezinfikuje aktivní infekci ihned poté, co byla detekována během provádění úlohy antivirové kontroly. Kaspersky Endpoint Security generuje aktivní události týkající se infekce v místních zprávách o aplikaci a na straně systému Kaspersky Security Center. Aktivní infekci lze dezinfikovat, když je úloha antivirové kontroly znovu spuštěna se zapnutou funkcí Pokročilá dezinfekce. Tímto způsobem může správce systému zvolit vhodný čas na provedení rozšířené dezinfekce a následně automaticky restartovat počítače.

Rozsah kontroly

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, pevný disk, vyměnitelný nebo síťový disk, složku nebo soubor.

V aplikaci Kaspersky Endpoint Security pro systém Windows 12.12 je z rozsahu kontroly aplikace vyloučen e-mail. Kontrolu příchozích a odchozích e-mailových zpráv provádí součást Ochrana před hrozbami v poště. Pokud používáte dřívější verzi modulu plug-in pro správu, aplikace vyloučí z rozsahu kontroly e-maily, i když je zásady zahrnují.

Plán kontrol

Manually. Režim spuštění, ve kterém můžete kontrolu spustit ručně v době, kdy je to pro vás výhodné.

By schedule. V tomto režimu spuštění úlohy kontroly bude aplikace spouštět úlohu kontroly podle vytvořeného plánu. Pokud je vybrán tento režim spuštění úlohy kontroly, je možné úlohu kontroly spustit i ručně.

Odložit spuštění úlohy po startu aplikace o N minut

Odložený start úlohy kontroly po spuštění aplikace. Při spouštění operačního systému běží mnoho procesů, proto je výhodné spuštění úlohy kontroly odložit a nespouštět ji ihned po spuštění aplikace Kaspersky Endpoint Security.

Spustit přeskočené úlohy

Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu, jakmile to bude možné. Úlohu lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače.

Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security přeskočené úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu.

Spustit pouze v době, kdy je počítač neaktivní

Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.

Spustit kontrolu jako

Ve výchozím nastavení je úloha kontroly spuštěna pod jménem uživatele, s jehož právy jste 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 aplikace, a úlohu kontroly spustit pod účtem tohoto uživatele.

Typy souborů

Aplikace Kaspersky Endpoint Security považuje soubory bez přípony za spustitelné soubory. Aplikace 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 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 zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje soubory podle jejich formátu. Kontrola souborů podle přípony je méně bezpečná, protože škodlivý soubor může mít příponu, která není na seznamu potenciálně infikovatelných (např. `.123`).

Kontrolovat pouze nové a upravené 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 soubor, který se kontroluje déle než N sekund

Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

Nespouštět více úloh kontroly najednou

Odložený start úloh kontroly, pokud již probíhá kontrola. Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače. Předpokládejme například, že aplikace spustila podle plánu úlohu Úplná kontrola. Pokud se uživatel pokusí spustit rychlou kontrolu z rozhraní aplikace, Kaspersky Endpoint Security tuto úlohu kontroly souborů zařadí do fronty a automaticky ji spustí po dokončení úlohy Úplná kontrola.

Aplikace Kaspersky Endpoint Security však okamžitě spustí úlohu kontroly, i když je spuštěna některá z následujících úloh kontroly:

- Kontrola vyměnitelných jednotek při připojení.
- Kontrola z místní nabídky.
- Kontrola kritických oblastí, která byla spuštěna před zjištěním indikátoru narušení (IoC).

Pokud toto políčko není zaškrtnuto, umožňuje aplikace Kaspersky Endpoint Security spustit více úloh kontroly současně. Prodádění více úloh kontroly vyžaduje více prostředků počítače.

Kontrolovat archivy

Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).

Kontrolovat distribuční balíčky

Kontrola distribučních balíčků aplikací 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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.

Kontrolovat soubory v poštovním formátu

Kontrola souborů ve formátu e-mailu a e-mailových databází. Aplikace kontroluje soubory PST a OST používané poštovními klienty MS Outlook a Windows Mail a také soubory EML.

Kaspersky Endpoint Security nepodporuje 64bitovou verzi poštovního klienta aplikace Microsoft Outlook. To znamená, že pokud je v počítači nainstalována 64bitová verze aplikace Microsoft Outlook, aplikace Kaspersky Endpoint Security nekontroluje soubory aplikace Microsoft Outlook (soubory PST a OST), i když je pošta součástí rozsahu kontroly.

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.

Pokud je v souborech PST nebo OST objeven škodlivý objekt, Kaspersky Endpoint Security ho v souladu s vybranou akcí (například dezinfekce nebo odstranění souboru) zneškodní.

Když je v souborech jiných poštovních klientů (například Mozilla Thunderbird) zjištěn škodlivý soubor, Kaspersky Endpoint Security pouze označí infikovanou zprávu. Zprávu s infikovanou přílohou je třeba odstranit ručně.

Kontrolovat archivy chráněné heslem

Je-li toto políčko zaškrtnuto, aplikace zkontroluje archivy chráněné heslem. Než bude možné soubory v archivu zkontrolovat, budete vyzváni k zadání hesla.

Pokud políčko zaškrtnuté není, aplikace přeskočí kontrolu archivů chráněných heslem.

Nerozbalovat velké složené soubory

Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu.

Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí.

Aplikace 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

(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).

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.

Jak nakonfigurovat spouštění kontroly vyměnitelných jednotek v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Místní úlohy** → **Kontrola vyměnitelných jednotek**.
4. V části **Akce při připojení vyměnitelné jednotky** v rozevíracím seznamu vyberte **Podrobná kontrola** nebo **Rychlá kontrola**.

5. Nakonfigurujte rozšířené možnosti pro kontrolu vyměnitelných jednotek (viz tabulka níže).
6. Uložte změny.

Jak nakonfigurovat spouštění kontroly vyměnitelných jednotek ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Removable Drives Scan**.
5. Pomocí přepínače **Removable Drives Scan ENABLED** můžete tuto součást povolit nebo zakázat.
6. V bloku **Scan type** vyberte položku **Detailed Scan** nebo **Quick Scan**.
7. Nakonfigurujte rozšířené možnosti pro kontrolu vyměnitelných jednotek (viz tabulka níže).
8. Uložte změny.

Jak nakonfigurovat spouštění kontroly vyměnitelných jednotek v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.
2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Pomocí přepínače **Kontrola vyměnitelných jednotek** můžete povolit nebo zakázat kontrolu vyměnitelných jednotek po připojení k počítači.
4. Nakonfigurujte rozšířené možnosti pro kontrolu vyměnitelných jednotek (viz tabulka níže).
5. Uložte změny.

Aplikace Kaspersky Endpoint Security tak spustí kontrolu vyměnitelných jednotek u vyměnitelných jednotek, které nejsou větší než zadaná maximální velikost. Pokud se úloha *Kontrola vyměnitelných jednotek* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

Nastavení úlohy Kontrola vyměnitelných jednotek

Parametr	Popis
Scan type	**Detailed Scan**. Je-li vybrána tato možnost, aplikace Kaspersky Endpoint Security při připojení vyměnitelné jednotky zkontroluje všechny soubory na vyměnitelné jednotce, včetně souborů vnořených ve složených objektech, archivů, distribučních balíčků a souborů ve formátech aplikací Office. Kaspersky Endpoint Security nekontroluje soubory ve formátu pošty ani archivy chráněné heslem. **Quick Scan**. Je-li vybrána tato možnost, po připojení vyměnitelné jednotky aplikace Kaspersky Endpoint Security zkontroluje pouze soubory v konkrétních formátech, které jsou na infekce nejnáchylnější, a nerozbalí složené objekty.
Maximum drive size (MB)	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security provede vybranou akci u vyměnitelných jednotek, jejichž velikost nepřekračuje maximální určenou velikost jednotky. Pokud velikost vyměnitelné jednotky přesáhne nakonfigurovanou hodnotu, aplikace Kaspersky Endpoint Security kontrolu přeskočí. Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security provede vybranou akci u vyměnitelných jednotek libovolné velikosti.
Hide scan progress bar	Pokud je toto políčko zaškrtnuto, bude aplikace Kaspersky Endpoint Security zobrazovat průběh kontroly vyměnitelných jednotek v samostatném okně a v části **Úlohy**. Jestliže je zaškrtnutí tohoto políčka zrušeno, bude aplikace Kaspersky Endpoint Security provádět kontrolu vyměnitelných jednotek na pozadí.
Prevent users from stopping the scan	Pokud je toto políčko zaškrtnuto, není pro úlohu kontroly vyměnitelných jednotek v místním rozhraní aplikace Kaspersky Endpoint Security k dispozici tlačítko **Zastavit** v části **Úlohy** a tlačítko **Zastavit** v okně kontroly vyměnitelných jednotek.

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.

Chcete-li ušetřit prostředky počítače, místo úlohy úplné kontroly se doporučuje používat úlohu kontroly na pozadí. Neovlivní to úroveň zabezpečení počítače. Tyto úlohy mají stejný rozsah kontroly. Z důvodu optimalizace zatížení počítače aplikace nespouští úlohu Úplná kontrola a úlohu Kontrola na pozadí současně. Pokud jste již spustili úlohu Úplná kontrola, aplikace Kaspersky Endpoint Security nebude spouštět úlohu Kontrola na pozadí po dobu sedmi dnů od dokončení úlohy Úplná kontrola.

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.

Jak povolit kontrolu na pozadí v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Místní úlohy** → **Kontrola na pozadí**.
4. Pomocí zaškrtávacího políčka **Povolit kontrolu na pozadí** povolte nebo zakažte kontroly na pozadí.
5. Uložte změny.

Jak povolit kontrolu na pozadí ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **File Threat Protection**.
5. V části **Background Scan** pomocí přepínače **Background Scan ENABLED** můžete kontrolu na pozadí povolit nebo zakázat.
6. Uložte změny.

Jak povolit kontrolu na pozadí v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.
2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.

3. Pomocí přepínače **Kontrola na pozadí** povolte nebo zakažte kontroly na pozadí.

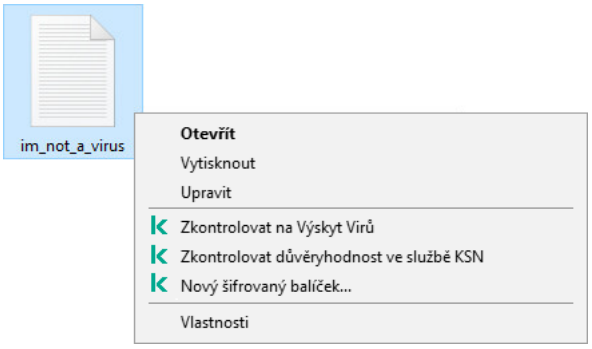
4. Uložte změny.

Pokud se úloha *Kontrola na pozadí* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

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

Jak nakonfigurovat kontrolu z místní nabídky v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Místní úlohy** → **Kontrola z místní nabídky**.
4. Nakonfigurujte kontrolu z místní nabídky (viz tabulka níže).
5. Uložte změny.

Jak nakonfigurovat kontrolu z místní nabídky ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **File Threat Protection**.
5. V části **Scan from Context Menu** nakonfigurujte kontrolu z místní nabídky (viz tabulka níže).
6. Uložte změny.

Jak nakonfigurovat kontrolu z místní nabídky v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.
2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Nakonfigurujte kontrolu z místní nabídky (viz tabulka níže).

4. Uložte změny.

Pokud se úloha *Kontrola z místní nabídky* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

Nastavení úlohy Kontrola z místní nabídky

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 aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Hloubková kontrola**. • **Doporučená**. Aplikace Kaspersky Endpoint Security kontroluje všechny typy souborů. Při kontrole složených souborů aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Střední kontrola**. • **Nízká**. Kaspersky Endpoint Security kontroluje pouze zadané formáty souborů. Při kontrole složených souborů aplikace kontroluje archivy, distribuční balíčky, soubory kancelářských formátů, ale nekontroluje archivy chráněné heslem. Když je nastavena tato úroveň zabezpečení, aplikace používá heuristickou analýzu s úrovní podrobností **Lehká kontrola**.
Akce při zjištění hrozby	**Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, 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.
Typy souborů	Aplikace Kaspersky Endpoint Security považuje soubory bez přípony za spustitelné soubory. Aplikace 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 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 zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje soubory podle jejich formátu. Kontrola souborů podle přípony je méně bezpečná, protože škodlivý soubor může mít příponu, která není na seznamu potenciálně infikovatelných (např. `.123`).
Kontrolovat pouze nové a upravené 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 soubor, který se kontroluje déle než N sekund	Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.
Kontrolovat archivy	Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).
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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
Kontrolovat soubory v poštovním formátu	Kontrola souborů ve formátu e-mailu a e-mailových databází. Aplikace kontroluje soubory PST a OST používané poštovními klienty MS Outlook a Windows Mail a také soubory EML.

Kaspersky Endpoint Security nepodporuje 64bitovou verzi poštovního klienta aplikace Microsoft Outlook. To znamená, že pokud je v počítači nainstalována 64bitová verze aplikace Microsoft Outlook, aplikace Kaspersky Endpoint Security nekontroluje soubory aplikace Microsoft Outlook (soubory PST a OST), i když je pošta součástí rozsahu kontroly.

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.

Pokud je v souborech PST nebo OST objeven škodlivý objekt, Kaspersky Endpoint Security ho v souladu s vybranou akcí (například dezinfekce nebo odstranění souboru) zneškodní.

Když je v souborech jiných poštovních klientů (například Mozilla Thunderbird) zjištěn škodlivý soubor, Kaspersky Endpoint Security pouze označí infikovanou zprávu. Zprávu s infikovanou přílohou je třeba odstranit ručně.

Kontrolovat archivy chráněné heslem

Je-li toto políčko zaškrtnuto, aplikace zkontroluje archivy chráněné heslem. Než bude možné soubory v archivu zkontrolovat, budete vyzváni k zadání hesla.

Pokud políčko zaškrtnuté není, aplikace přeskočí kontrolu archivů chráněných heslem.

Nerozbalovat velké složené soubory

Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu.

Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí.

Aplikace 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 integrity aplikace

Aplikace Kaspersky Endpoint Security zkontroluje moduly aplikace z hlediska změn nebo poškození. Pokud má například knihovna aplikace nesprávný digitální podpis, je považována za poškozenou. Úloha *Kontrola integrity aplikací* je určena ke kontrole souborů aplikací. Úlohu *Kontrola integrity aplikací* spusťte, pokud aplikace Kaspersky Endpoint Security zjistila škodlivý objekt, ale neneutralizovala ho.

Úlohu *Kontrola integrity aplikací* můžete vytvořit jak ve webové konzole aplikace Kaspersky Security Center, 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.

Jak provést kontrolu integrity aplikace prostřednictvím konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Kontrola integrity aplikací**.

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 **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. Kaspersky Endpoint Security zkontroluje integritu aplikace. Případně můžete ve vlastnostech úlohy nakonfigurovat plán kontroly integrity aplikace (viz tabulka níže).

[Jak provést kontrolu integrity aplikace prostřednictvím webové konzoly]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Application Integrity Check**.
   c. Do pole **Task name** zadejte stručný popis, například *Kontrola integrity aplikace po infekci počítače*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Zaškrtněte políčko vedle úlohy.

Kaspersky Endpoint Security zkontroluje integritu aplikace. Případně můžete ve vlastnostech úlohy nakonfigurovat plán kontroly integrity aplikace (viz tabulka níže).

[*Jak spustit kontrolu integrity v rozhraní aplikace*]

1. V hlavním okně aplikace přejděte do části **Úlohy**.

2. Otevře se seznam úloh; vyberte úlohu *Kontrola integrity aplikací* a klikněte na **Spustit**.

Kaspersky Endpoint Security zkontroluje integritu aplikace. Případně můžete ve vlastnostech úlohy nakonfigurovat plán kontroly integrity aplikace (viz tabulka níže). Pokud se úloha *Kontrola integrity aplikací* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

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. **Podle plánu**. V tomto režimu spuštění úlohy kontroly bude aplikace spouštět úlohu kontroly podle vytvořeného plánu. Pokud je vybrán tento režim spuštění úlohy kontroly, je možné úlohu kontroly spustit i ručně.
Spustit přeskočené úlohy	Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu, jakmile to bude možné. Úlohu lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače. Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security přeskočené úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu.
Spustit pouze v době, kdy je počítač neaktivní	Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.

Úprava rozsahu kontroly

Rozsah kontroly je seznam cest ke složkám a cest, které aplikace Kaspersky Endpoint Security kontroluje při provádění úlohy. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

Chcete-li upravit rozsah kontroly, doporučujeme použití úlohy *Vlastní kontrola*. Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Úplná kontrola* a *Kontrola kritických oblastí*.

Aplikace Kaspersky Endpoint Security má v rozsahu kontroly následující předdefinované objekty:

- **Systémová paměť**.
- **Běžící procesy a Spouštěcí objekty**.

  Paměť obsazená procesy a spustitelnými soubory aplikace, které jsou spuštěny při spuštění systému.
- **Spouštěcí sektory disku**.

  Spouštěcí sektory pevného disku a vyměnitelného disku.
- **Záloha systému**.

  Obsah složky s informacemi o systémovém svazku.
- **Všechna externí zařízení**.
- **Všechny pevné disky**.
- **Všechny síťové jednotky**.

  V aplikaci Kaspersky Endpoint Security pro systém Windows 12.12 je z rozsahu kontroly aplikace vyloučen e-mail. Kontrolu příchozích a odchozích e-mailových zpráv provádí součást Ochrana před hrozbami v poště. Pokud používáte dřívější verzi modulu plug-in pro správu, aplikace vyloučí z rozsahu kontroly e-maily, i když je zásady zahrnují.

  Doporučujeme vytvořit samostatnou úlohu kontroly pro kontrolu síťových disků nebo sdílených složek. V nastavení úlohy *Kontrola malwaru* zadejte uživatele, který má přístup k zápisu na tuto jednotku; je to nezbytné pro zmírnění dopadů zjištěných hrozeb. Pokud má server, na kterém se nachází síťová jednotka, vlastní nástroje zabezpečení, nespouštějte úlohu kontroly pro tuto jednotku. Vyhnete se tak dvojí kontrole objektu a zlepšíte výkon serveru.

Chcete-li z rozsahu kontroly vyloučit složky nebo soubory, přidejte složku nebo soubor do důvěryhodné zóny.

Jak upravit rozsah kontroly v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Vyberte úlohu kontroly a dvojitým kliknutím otevřete vlastnosti této úlohy.
   V případě potřeby vytvořte úlohu *Kontrola malwaru*.
4. V okně vlastností úlohy vyberte část **Nastavení**.
5. V části **Rozsah kontroly** klikněte na tlačítko **Nastavení**.
6. V okně, které se otevře, vyberte objekty, které chcete přidat do rozsahu kontroly nebo z něj vyloučit.
7. Pokud chcete do rozsahu kontroly přidat nový objekt:
   a. Klikněte na tlačítko **Přidat**.
   b. Do pole **Objekt** zadejte cestu ke složce nebo souboru.
      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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

      Masky můžete použít kdekoli v cestě k souboru nebo složce. Chcete-li například, aby rozsah kontroly zahrnoval složku Stažené soubory pro všechny uživatelské účty v počítači, zadejte masku `C:\Users\*\Downloads\`.

      Objekt **Tento počítač** v seznamu souborových prostředků počítače obsahuje následující objekty: **Všechny pevné disky**, **Všechny síťové jednotky** a **Všechny vyměnitelné jednotky**.

   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. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak upravit rozsah kontroly ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na úlohu kontroly.
   Otevře se okno vlastností úlohy. V případě potřeby vytvořte úlohu *Malware Scan*.
3. Vyberte kartu **Application settings**.
4. V části **Scan scope** vyberte objekty, které chcete přidat do rozsahu kontroly nebo z něj vyloučit.
5. Pokud chcete do rozsahu kontroly přidat nový objekt:
   a. Klikněte na tlačítko **Add**.
   b. Zadejte cestu k souboru nebo složce.
      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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

Masky můžete použít kdekoli v cestě k souboru nebo složce. Chcete-li například, aby rozsah kontroly zahrnoval složku Stažené soubory pro všechny uživatelské účty v počítači, zadejte masku `C:\Users\*\Downloads\`.

Objekt můžete z kontroly vyloučit, aniž byste jej odstranili ze seznamu objektů v rozsahu kontroly. Chcete-li to provést, přepněte přepínač vedle něj do polohy vypnuto.

6. Uložte změny.

Jak upravit rozsah kontroly v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.
2. Otevře se seznam úloh; vyberte úlohu *Vlastní kontrola* a klikněte na **Vybrat**.

   Rozsah kontroly můžete také upravit pro jiné úlohy. Odborníci společnosti Kaspersky doporučují, abyste neměnili rozsah kontroly úlohy *Úplná kontrola* a *Kontrola kritických oblastí*.
3. V okně, které se otevře, vyberte objekty, které chcete přidat do rozsahu kontroly.
4. Uložte změny.

Pokud se úloha kontroly nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

Spuštění naplánované kontroly

Kontrola malwaru pomocí úlohy *Kontrola malwaru* může být časově náročná a může zvýšit využití počítačových zdrojů aplikací Kaspersky Endpoint Security. Proto doporučujeme vybrat optimální dobu spuštění úlohy, aby byl dopad na výkon ostatních aplikací minimalizován.

Pokud například zaměstnanci ve vaší organizaci pracují podle pevného plánu, můžete nakonfigurovat kontrolu počítače tak, aby se spouštěla v noci nebo o víkendech. Pokud z jakéhokoli důvodu nelze úlohu spustit (například, když je počítač vypnutý), můžete nakonfigurovat automatické spuštění vynechané úlohy ihned, jakmile to bude možné. Tuto funkci je třeba používat s opatrností, protože může zpomalovat aplikace při ranním zapnutí počítače uživatele.

Pokud nemůžete určit optimální plán kontroly, který by vyhovoval vašim potřebám, můžete kontrolu nakonfigurovat tak, aby se spustila v případě splnění jedné z následujících zvláštních podmínek:

- Po aktualizaci databáze.

  Aplikace Kaspersky Endpoint Security spustí kontrolu počítače s aktualizovanými databázemi podpisů.

- Po spuštění aplikace.

  Aplikace Kaspersky Endpoint Security spustí kontrolu počítače, když po spuštění aplikace uplyne určitá doba. Při spouštění operačního systému běží mnoho procesů, proto je výhodné spuštění úlohy kontroly odložit a nespouštět ji ihned po spuštění aplikace Kaspersky Endpoint Security.

- Funkce Wake-on-LAN.

  Aplikace Kaspersky Endpoint Security spouští kontrolu počítače podle plánu, i když je počítač vypnutý. K tomu aplikace používá funkci Wake-on-LAN operačního systému. Funkce Wake-on-LAN umožňuje vzdálené napájení počítače odesláním speciálního signálu po místní síti. Chcete-li tuto funkci používat, musíte v nastavení systému BIOS povolit Wake-on-LAN.

  Spuštění kontroly pomocí Wake-on-LAN můžete nakonfigurovat pouze pro úlohu *Kontrola malwaru* v aplikaci Kaspersky Security Center. Službu Wake-on-LAN nelze povolit pro kontrolu počítače v rozhraní aplikace.

- V době, kdy počítač není aktivní.

  Když je spořič obrazovky aktivní nebo je obrazovka uzamčena, aplikace Kaspersky Endpoint Security spouští kontrolu počítače podle plánu. Pokud uživatel odemkne počítač, Kaspersky Endpoint Security kontrolu pozastaví. V tomto případě může dokončení úplné kontroly trvat několik dní.

- Když byla úloha přeskočena.

  Aplikace Kaspersky Endpoint Security spustí přeskočenou úlohu, co nejdříve to bude možné. Úlohu lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače.

Jak konfigurovat plán kontrol ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu kontroly.

   Otevře se okno vlastností úlohy.

3. V okně vlastností úlohy vyberte kartu **Schedule**.

4. Nakonfigurujte plán úloh kontroly.

5. V závislosti na vybrané frekvenci proveďte rozšířené nastavení pro plán spouštění úlohy (viz tabulka níže).

6. Uložte změny.

Jak konfigurovat plán kontrol v rozhraní aplikace

Plán kontroly můžete konfigurovat pouze v případě, že v počítači nejsou použity zásady. U počítačů se zásadami můžete nakonfigurovat plán úlohy *Kontrola malwaru* v aplikaci Kaspersky Security Center.

1. V hlavním okně aplikace přejděte do části **Úlohy**.

2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.

   Můžete nakonfigurovat plán pro spouštění úplné kontroly, kontroly kritických oblastí nebo kontroly integrity. Vlastní kontrolu můžete spustit pouze ručně.

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 (viz tabulka níže).

6. Uložte změny.

Nastavení plánu kontrol

Parametr	Popis
Plán kontrol	**Ručně**. Režim spuštění, ve kterém můžete kontrolu spustit ručně v době, kdy je to pro vás výhodné. **Podle plánu**. V tomto režimu spuštění úlohy kontroly bude aplikace spouštět úlohu kontroly podle vytvořeného plánu. Pokud je vybrán tento režim spuštění úlohy kontroly, je možné úlohu kontroly spustit i ručně.
Odložit spuštění úlohy po startu aplikace o N minut	Odložený start úlohy kontroly po spuštění aplikace. Při spouštění operačního systému běží mnoho procesů, proto je výhodné spuštění úlohy kontroly odložit a nespouštět ji ihned po spuštění aplikace Kaspersky Endpoint Security.
Spustit přeskočené úlohy	Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu, jakmile to bude možné. Úlohu lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače. Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security přeskočené úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu.
Spustit pouze v době, kdy je počítač neaktivní	Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.
Use automatically randomized delay for task starts *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Pokud toto políčko zaškrtnuto, úloha se nespustí striktně podle plánu, ale náhodně v určitém intervalu, to znamená, že se rozloží její počáteční časy. Náhodné časy spuštění pomáhají vyhnout se velkému počtu počítačů současně přistupujících k administračnímu serveru, když je úloha spuštěna podle plánu. Rozsah náhodných časů spuštění se automaticky vypočítá při vytvoření úlohu v závislosti na počtu počítačů, které mají tuto úlohu přiřazenu. Následně je úloha vždy spuštěna ve vypočítaném čase zahájení. Kdykoli se však změní nastavení úlohy nebo je spuštěna ručně, vypočítaný čas zahájení se změní. Pokud toto políčko není zaškrtnuto, úloha se spustí přesně v naplánovaném čase.

Use randomized delay for task starts within an interval of (min)	Je-li toto políčko zaškrtnuto, úloha se spouští v počítačích v náhodnou dobu v určitém časovém rámci. Náhodné časy spuštění pomáhají vyhnout se velkému počtu počítačů současně přistupujících k administračnímu serveru, když je úloha spuštěna podle plánu. Pokud toto políčko není zaškrtnuto, úloha se spustí přesně v naplánovaném čase.
Stop the task if it runs longer than (min) *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu. Chcete-li zkrátit dobu provádění úlohy, můžete např. nakonfigurovat rozsah kontroly nebo optimalizovat kontrolu.
Turn on devices by using the Wake-on-LAN function before starting the task (min) *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Pokud je toto políčko zaškrtnuto, operační systém počítače dostane zadanou dobu přípravy k dokončení spouštění před spuštěním úlohy. Výchozí hodnota doby přípravy je 5 minut. Zaškrtněte políčko, pokud chcete úlohu spustit na všech počítačích, včetně vypnutých počítačů.
Shut down the devices after completing the task *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Tuto funkci můžete například povolit za účelem kontroly počítače v pátek po pracovní době. Po dokončení úlohy aplikace vypne počítač na víkend.

Spuštění kontroly jako jiný uživatel

Ve výchozím nastavení je úloha kontroly spuštěna pod jménem uživatele, s jehož právy jste 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 aplikace, a úlohu kontroly spustit pod účtem tohoto uživatele.

Následující kontroly můžete spustit jako jiný uživatel:

- Kontrola kritických oblastí,
- Úplná kontrola,
- Vlastní kontrola,
- Kontrola z místní nabídky.

Pro spuštění kontroly vyměnitelných jednotek, kontroly na pozadí a kontroly integrity nemůžete konfigurovat uživatelská práva.

Jak spustit kontrolu jako jiný uživatel 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 **Tasks**.
4. Vyberte úlohu kontroly a dvojitým kliknutím otevřete vlastnosti této úlohy.
5. V okně vlastností úlohy vyberte část **Account**.
6. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy kontroly.
7. Uložte změny.

Jak spustit kontrolu jako jiný uživatel ve webové konzole nebo cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na úlohu kontroly.
   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Settings**.

4. V bloku **Account** klikněte na tlačítko **Settings**.
5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy kontroly.
6. Uložte změny.

Jak spustit kontrolu jako jiný uživatel v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.
2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.
3. Ve vlastnostech úlohy vyberte možnosti **Rozšířené nastavení** → **Spustit kontrolu jako**.
4. V okně, které se otevře, zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy kontroly.
5. Uložte změny.

Pokud se úloha kontroly nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

Optimalizace kontroly

Omezení využití CPU při kontrole počítače

Můžete omezit využití CPU při provádění úlohy *Kontrola malwaru*. To může prodloužit dobu potřebnou ke kontrole počítače.

Jak omezit využití CPU při kontrole počítače v konzole pro správu (MMC)

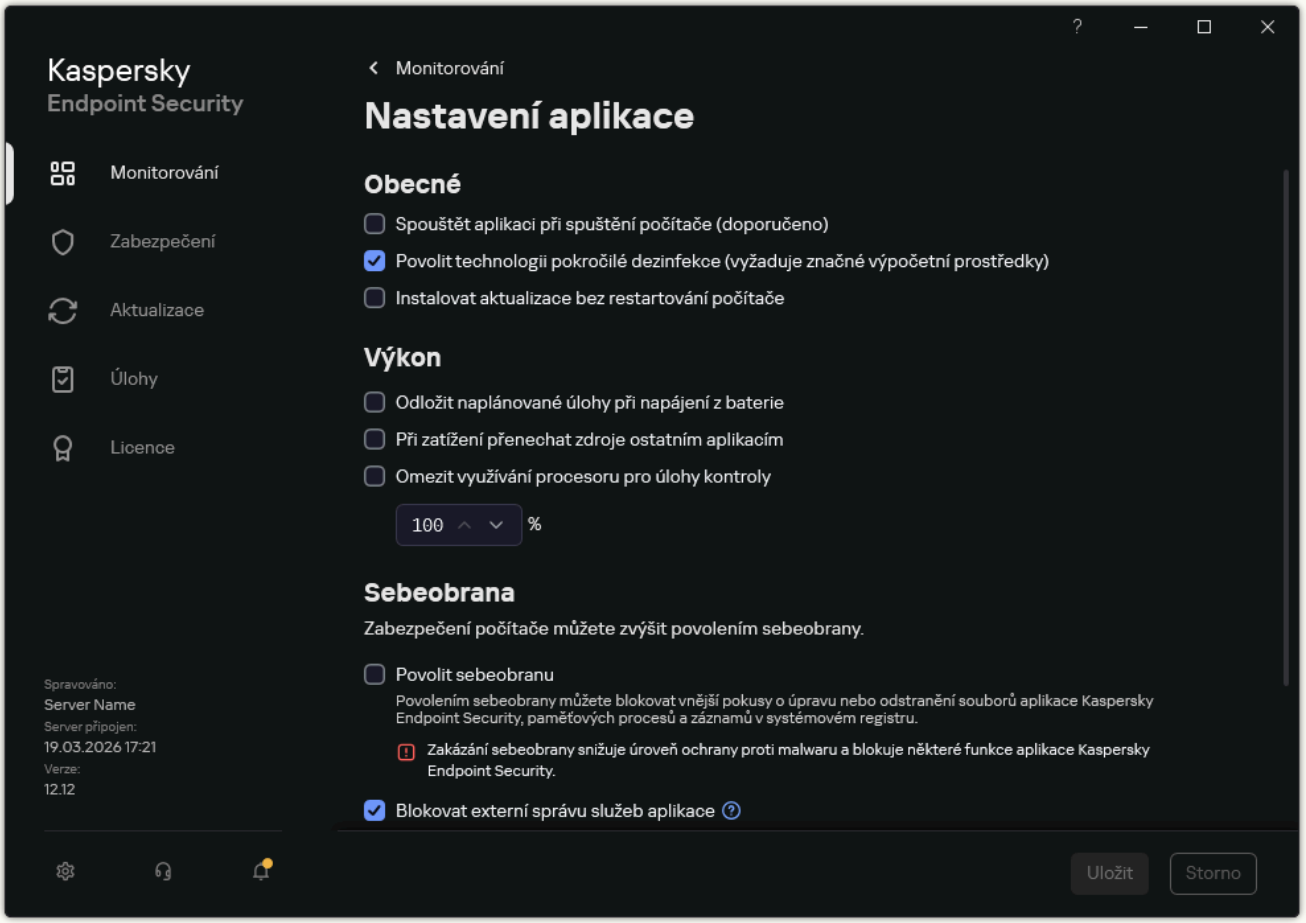
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V části **Výkon** zaškrtněte políčko **Omezit využívání procesoru pro úlohy kontroly** a zadejte průměrnou hodnotu spotřeby prostředků CPU v procentech.
5. Uložte změny.

Jak omezit využití CPU při kontrole počítače ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Performance**.
5. V části **Limit CPU usage for scan tasks** přepněte přepínač na **Limit CPU usage for scan tasks** a zadejte průměrnou hodnotu spotřeby prostředků CPU v procentech.
6. Uložte změny.

Jak omezit využití CPU při kontrole počítače v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. V části **Výkon** zaškrtněte políčko **Omezit využívání procesoru pro úlohy kontroly** a zadejte průměrnou hodnotu spotřeby prostředků CPU v procentech.

4. Uložte změny.

Konfigurace rozšířeného nastavení úlohy pro úlohu Kontrola malwaru.

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).

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.

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

Jak optimalizovat kontroly v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve stromu konzoly vyberte možnost **Tasks**.

3. Vyberte úlohu kontroly a dvojitým kliknutím otevřete vlastnosti této úlohy.
   V případě potřeby vytvořte úlohu *Kontrola malwaru*.

4. V okně vlastností úlohy vyberte část **Nastavení**.

5. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
   Toto tlačítko slouží k otevření okna nastavení úlohy.

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

- **Kontrolovat pouze nové a upravené 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.

  Můžete také nakonfigurovat kontrolu nových souborů podle typu. Můžete například kontrolovat všechny distribuční balíčky a kontrolovat pouze nové archivy a soubory formátu Office.

- **Přeskočit soubory, které se kontrolují déle než N s**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

- **Nespouštět více úloh kontroly najednou**. Odložený start úloh kontroly, pokud již probíhá kontrola. Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače. Předpokládejme například, že aplikace spustila podle plánu úlohu Úplná kontrola. Pokud se uživatel pokusí spustit rychlou kontrolu z rozhraní aplikace, Kaspersky Endpoint Security tuto úlohu kontroly souborů zařadí do fronty a automaticky ji spustí po dokončení úlohy Úplná kontrola.

7. Klikněte na tlačítko **Rozšířené**.

   Toto tlačítko slouží k otevření okna nastavení kontroly složených souborů.

8. V bloku **Omezení velikosti** zaškrtněte políčko **Nerozbalovat velké složené soubory**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

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

9. Klikněte na tlačítko **OK**.

10. Přejděte na kartu **Další**.

11. 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).

12. Uložte změny.

[Jak optimalizovat kontrolu ve webové konzole a cloudové konzole](#)

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu kontroly.

   Otevře se okno vlastností úlohy. V případě potřeby vytvořte úlohu *Malware Scan*.

3. Vyberte kartu **Application settings**.

4. V bloku **Action on threat detection** zaškrtněte políčko **Scan only new and modified files**. 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.

   Můžete také nakonfigurovat kontrolu nových souborů podle typu. Můžete například kontrolovat všechny distribuční balíčky a kontrolovat pouze nové archivy a soubory formátu Office.

5. V bloku **Scan optimization** zaškrtněte políčko **Do not unpack large compound files**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

   Aplikace Kaspersky Endpoint Security kontroluje velké soubory extrahované z archivů bez ohledu na to, zda je či není zaškrtnuto políčko **Do not unpack large compound files**.

6. Zaškrtněte políčko **Do not run multiple scan tasks at the same time**. Odložený start úloh kontroly, pokud již probíhá kontrola. Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače.

Předpokládejme například, že aplikace spustila podle plánu úlohu Úplná kontrola. Pokud se uživatel pokusí spustit rychlou kontrolu z rozhraní aplikace, Kaspersky Endpoint Security tuto úlohu kontroly souborů zařadí do fronty a automaticky ji spustí po dokončení úlohy Úplná kontrola.

7. V bloku **Advanced settings** zaškrtněte políčko **Skip file that is scanned for longer than (sec)**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

8. Uložte změny.

Jak optimalizovat kontrolu v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Úlohy**.

2. V seznamu vyberte úlohu kontroly a klikněte na tlačítko ⚙.

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

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

   - **Kontrolovat pouze nové a upravené 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.

     Můžete také nakonfigurovat kontrolu nových souborů podle typu. Můžete například kontrolovat všechny distribuční balíčky a kontrolovat pouze nové archivy a soubory formátu Office.

   - **Přeskočit soubor, který se kontroluje déle než N sekund**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

   - **Nespouštět více úloh kontroly najednou**. Odložený start úloh kontroly, pokud již probíhá kontrola. Pokud aktuální kontrola pokračuje, Kaspersky Endpoint Security zařadí nové úlohy kontroly do fronty. To pomáhá optimalizovat zátěž počítače. Předpokládejme například, že aplikace spustila podle plánu úlohu Úplná kontrola. Pokud se uživatel pokusí spustit rychlou kontrolu z rozhraní aplikace, Kaspersky Endpoint Security tuto úlohu kontroly souborů zařadí do fronty a automaticky ji spustí po dokončení úlohy Úplná kontrola.

5. V bloku **Omezení velikosti** zaškrtněte políčko **Nerozbalovat velké složené soubory**. Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.

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

6. 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).

7. Uložte změny.

Pokud se úloha kontroly nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

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.

Aktualizační funkce (včetně poskytování aktualizací antivirových signatur a aktualizací báze kódů) nemusí být v softwaru dostupná na území USA.

Pravidelné aktualizace vyžadují platnou licenci. Pokud nemáte k dispozici žádnou licenci, aktualizaci budete moci provést jen jednou.

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.

Pokud jsou databáze zastaralé, balíček aktualizace může být velký, což může způsobit dodatečný internetový provoz (až několik desítek MB).

Informace o aktuálním stavu databází Kaspersky Endpoint Security se zobrazují v hlavním okně aplikace nebo v popisku, který se zobrazí, když umístíte kurzor na ikonu aplikace v oznamovací oblasti.

Informace o výsledcích aktualizace a všech událostech, k nimž dojde během aktualizace, jsou zaznamenávány do zprávy aplikace Kaspersky Endpoint Security.

Pokud aplikace funguje v režimu Light Agent, při aktualizaci databází a modulů aplikace je třeba brát zvláštní ohledy.

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:

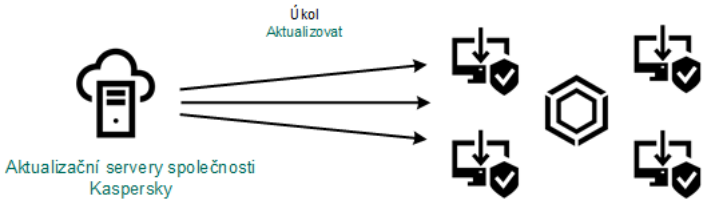
- Antivirové databáze. Antivirové databáze obsahují databáze signatur malwaru, popis síťových útoků, databáze škodlivých a phishingových webových adres, databáze reklamních lišt, databáze nevyžádané pošty a další data.

- 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 *Download updates to the Administration Server repository*.

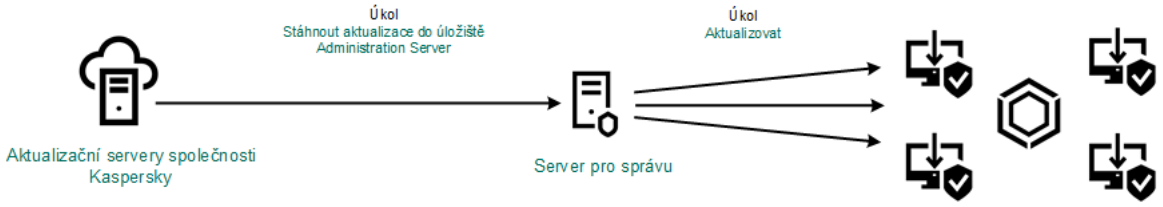
2. Stáhněte balíček aktualizace do sdílené složky (volitelné).

   Balíček aktualizace můžete do úložiště stáhnout následujícími způsoby:

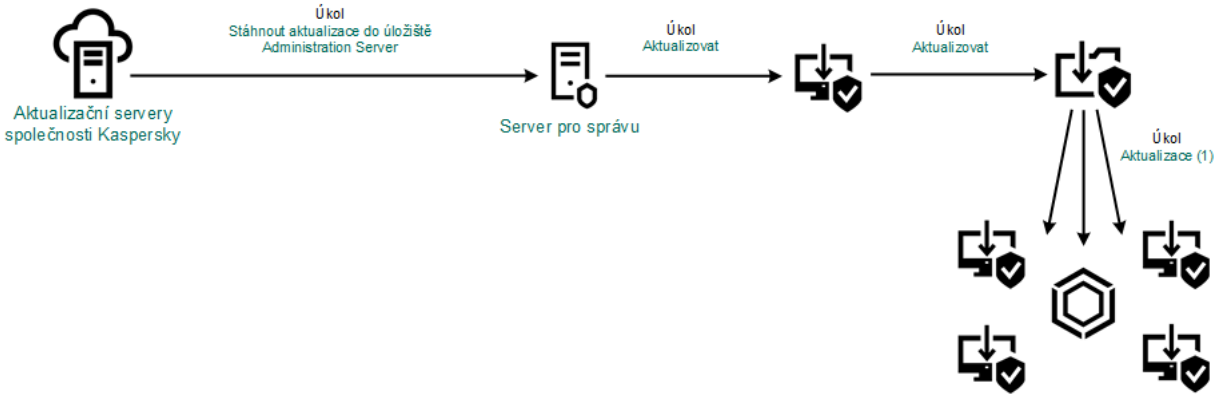
   - Pomocí úlohy *Aktualizace databází a modulů aplikace* v aplikaci Kaspersky Endpoint Security. Úloha je určena pro některý z počítačů v místní firemní síti.
   - Pomocí nástroje Kaspersky Update Utility. Podrobné informace o použití nástroje Kaspersky Update Utility najdete ve znalostní bázi společnosti Kaspersky.

3. Proveďte distribuci aktualizačního balíčku do klientských počítačů.

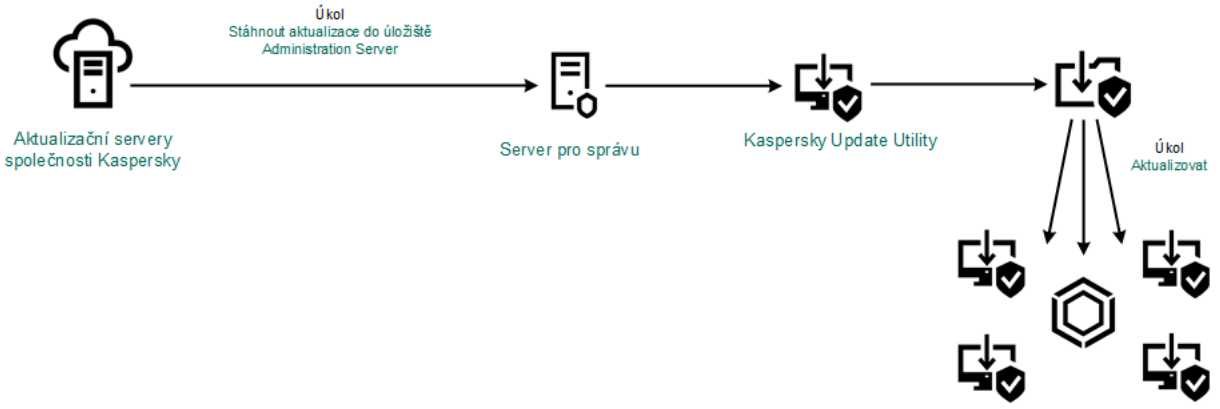
   Aktualizační balíček je distribuován do klientských počítačů pomocí úlohy *Aktualizace databází a modulů aplikace* v aplikaci Kaspersky Endpoint Security. Můžete vytvořit neomezený počet úloh aktualizací pro každou skupinu správy.



Aktualizace ze serverového úložiště



Aktualizace ze sdílené složky



Aktualizace pomocí nástroje Kaspersky Update Utility

U aplikace Kaspersky Security Center 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 stahování aktualizačního balíčku do úložiště serveru pro správu (úloha *Download updates to the Administration Server repository*).

   Úloha *Download updates to the Administration Server repository* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu a tato úloha může mít pouze jednu jedinou instanci. Ve výchozím nastavení aplikace Kaspersky Security Center zkopíruje aktualizační balíček do složky `\\<server name>\KLSHARE\Updates`. Další informace o stahování aktualizací do úložiště serveru pro správu najdete v nápovědě k aplikaci Kaspersky Security Center.

2. Nakonfigurujte aktualizace databází a modulů aplikace z určeného serverového úložiště do zbývajících počítačů v síti LAN organizace (úloha *Aktualizace databází a modulů aplikace*).

   Jak nakonfigurovat aktualizaci aplikace Kaspersky Endpoint Security ze zadaného úložiště serveru v konzole pro správu (MMC)

   1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

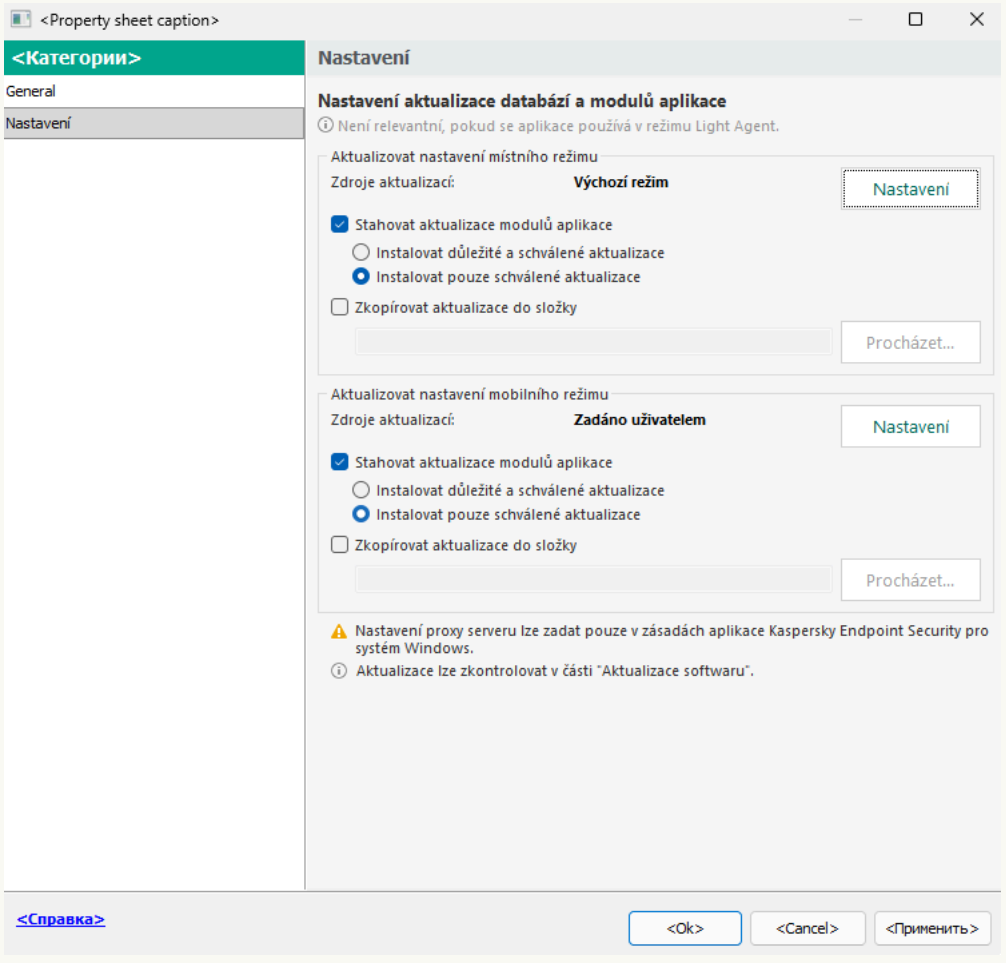
      Ve stromu konzoly vyberte možnost **Tasks**.

   2. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

      Otevře se okno vlastností úlohy.

      Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

   3. V okně vlastností úlohy vyberte část **Settings**.



Nastavení úlohy Aktualizace databází a modulů aplikace

   4. V bloku **Aktualizovat nastavení místního režimu** klikněte na tlačítko **Nastavení**.

   5. V seznamu zdrojů aktualizací se ujistěte, že je povolena aktualizace ze zdroje **Kaspersky Security Center**. Kromě toho musí mít zdroj **Kaspersky Security Center** nejvyšší prioritu.

   6. V případě potřeby přidejte zdroje aktualizací:

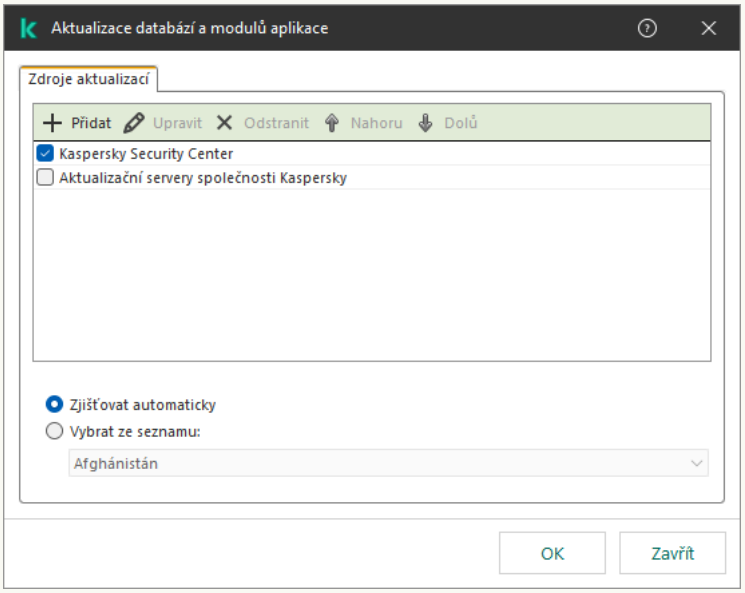
      a. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.

b. V poli **Zdroje aktualizací** 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 aktualizací se musí shodovat s adresou zadanou v poli **Folder for storing updates** při konfiguraci stažení aktualizací do serverového úložiště (úloha *Download updates to the Administration Server repository*).

c. Klikněte na tlačítko **OK**.

Zdroj aktualizací můžete vyloučit, aniž byste jej odebírali ze seznamu zdrojů aktualizací. Chcete-li tak učinit, zrušte zaškrtnutí políčka vedle objektu.



Zdroje aktualizace

7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

8. V okně vlastností úlohy vyberte část **Schedule** a nakonfigurujte režim spuštění úlohy.

9. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu v ručním režimu.

10. Uložte změny.

Jak nakonfigurovat aktualizaci aplikace Kaspersky Endpoint Security ze zadaného úložiště serveru ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Update** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Update* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Update*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Application settings** → **Local mode**.

4. V seznamu zdrojů aktualizací se ujistěte, že je povolena aktualizace ze zdroje **Kaspersky Security Center**. Kromě toho musí mít zdroj **Kaspersky Security Center** nejvyšší prioritu.

5. V případě potřeby přidejte zdroje aktualizací:

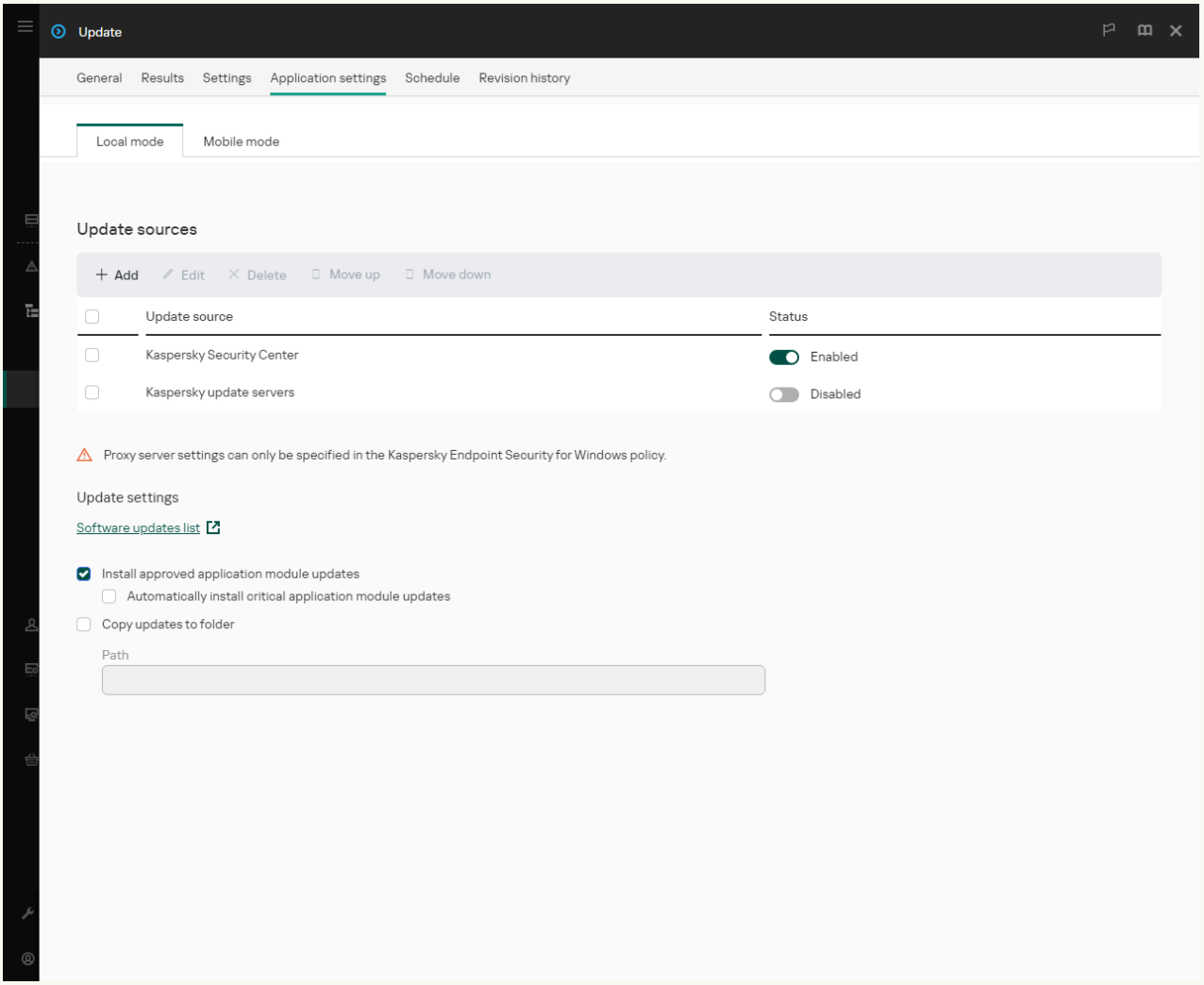
   a. V seznamu zdrojů aktualizací klikněte na tlačítko **Add**.

   b. V poli **Update sources** 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 aktualizací se musí shodovat s adresou zadanou v poli **Folder for storing updates** při konfiguraci stažení aktualizací do serverového úložiště (úloha *Download updates to the Administration Server repository*).

c. Klikněte na tlačítko **Save**.

Zdroj aktualizací můžete vyloučit, aniž byste jej odebírali ze seznamu zdrojů aktualizací. Chcete-li to provést, přepněte přepínač vedle něj do polohy vypnuto.



Zdroje aktualizace

6. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Up** a **Down**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

7. V okně vlastností úlohy vyberte část **Schedule** a nakonfigurujte režim spuštění úlohy.

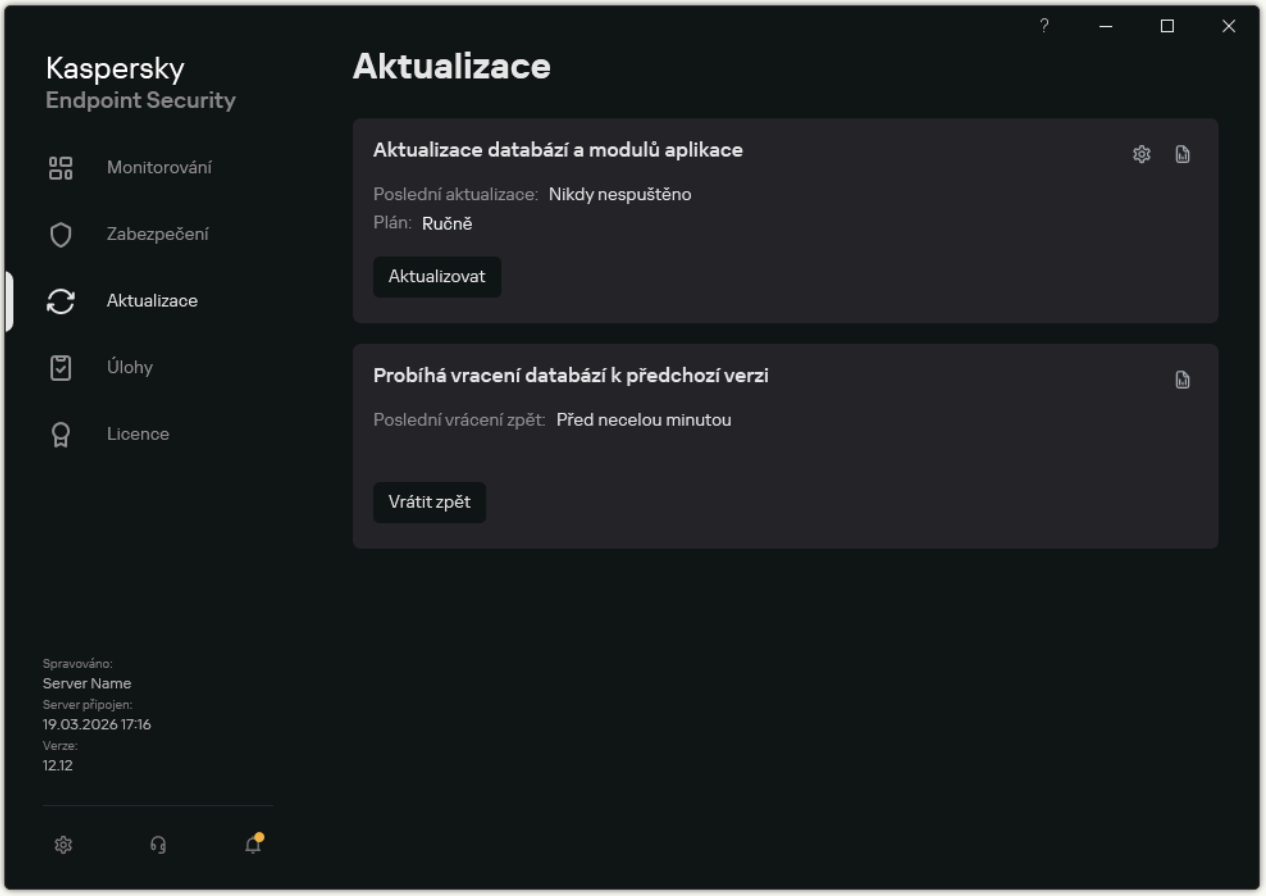
8. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu v ručním režimu.

9. Uložte změny.

[Jak nakonfigurovat aktualizaci aplikace Kaspersky Endpoint Security ze zadaného úložiště serveru ve webové konzole]

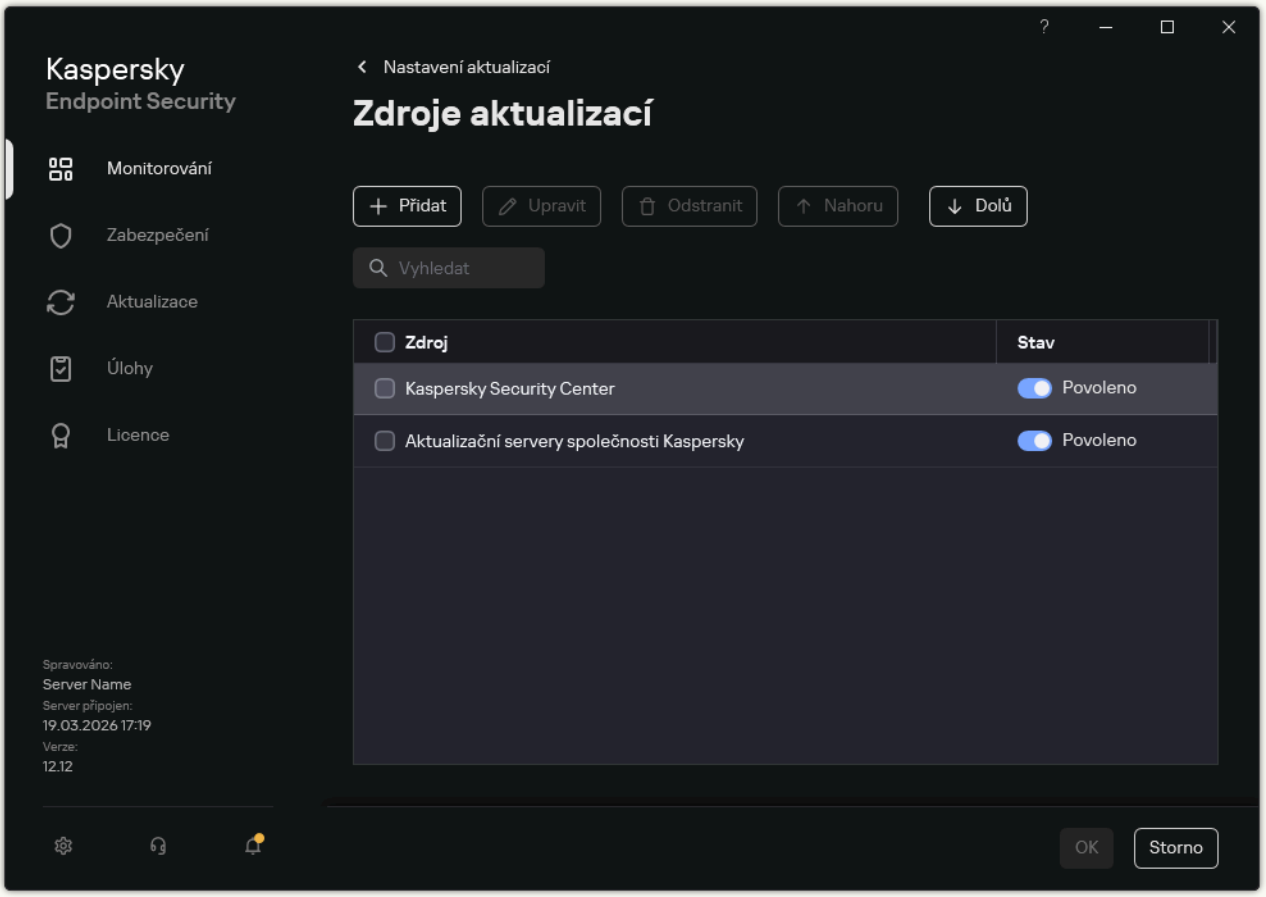
Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.
   Otevře se okno vlastností úlohy.
3. V okně vlastností úlohy klikněte na možnost **Vybrat zdroje aktualizací**.
4. V seznamu zdrojů aktualizací se ujistěte, že je povolena aktualizace ze zdroje **Kaspersky Security Center**. Kromě toho musí mít zdroj **Kaspersky Security Center** nejvyšší prioritu.
5. V případě potřeby přidejte zdroje aktualizací:
   a. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.



Zdroje aktualizace

a. 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 aktualizací se musí shodovat s adresou zadanou v poli **Folder for storing updates** při konfiguraci stažení aktualizací do serverového úložiště (úloha *Download updates to the Administration Server repository*).

b. Klikněte na tlačítko **Vybrat**.

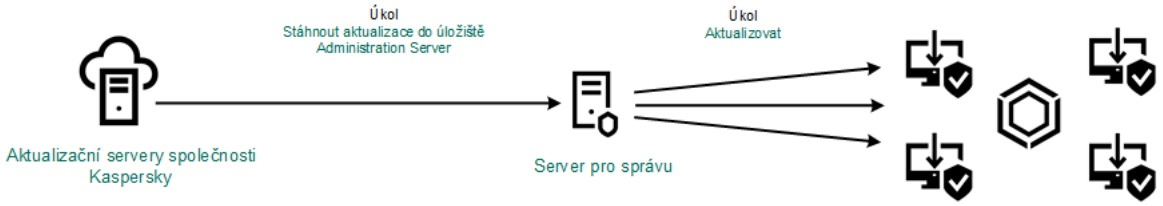
Zdroj aktualizací můžete vyloučit, aniž byste jej odebírali ze seznamu zdrojů aktualizací. Chcete-li to provést, přepněte přepínač vedle něj do polohy vypnuto.

6. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

> Pokud je počítač spravován aplikací Kaspersky Security Center, není možné konfigurovat režim spuštění pro úlohu *Aktualizace databází a modulů aplikace*. Úlohu můžete spustit pouze ručně.

7. Uložte změny.



Aktualizace ze serverového úložiště

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.

Verze a lokalizace aplikace Kaspersky Endpoint Security, která zkopíruje aktualizační balíček do sdílené složky, musí odpovídat verzi a lokalizaci aplikace, která aktualizuje databáze ze sdílené složky. Pokud se verze nebo lokalizace aplikací neshodují, může aktualizace databáze skončit chybou.

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.

   Jak povolit kopírování aktualizačního balíčku do sdílené složky v konzole pro správu (MMC)

   1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
   2. Ve stromu konzoly vyberte možnost **Tasks**.

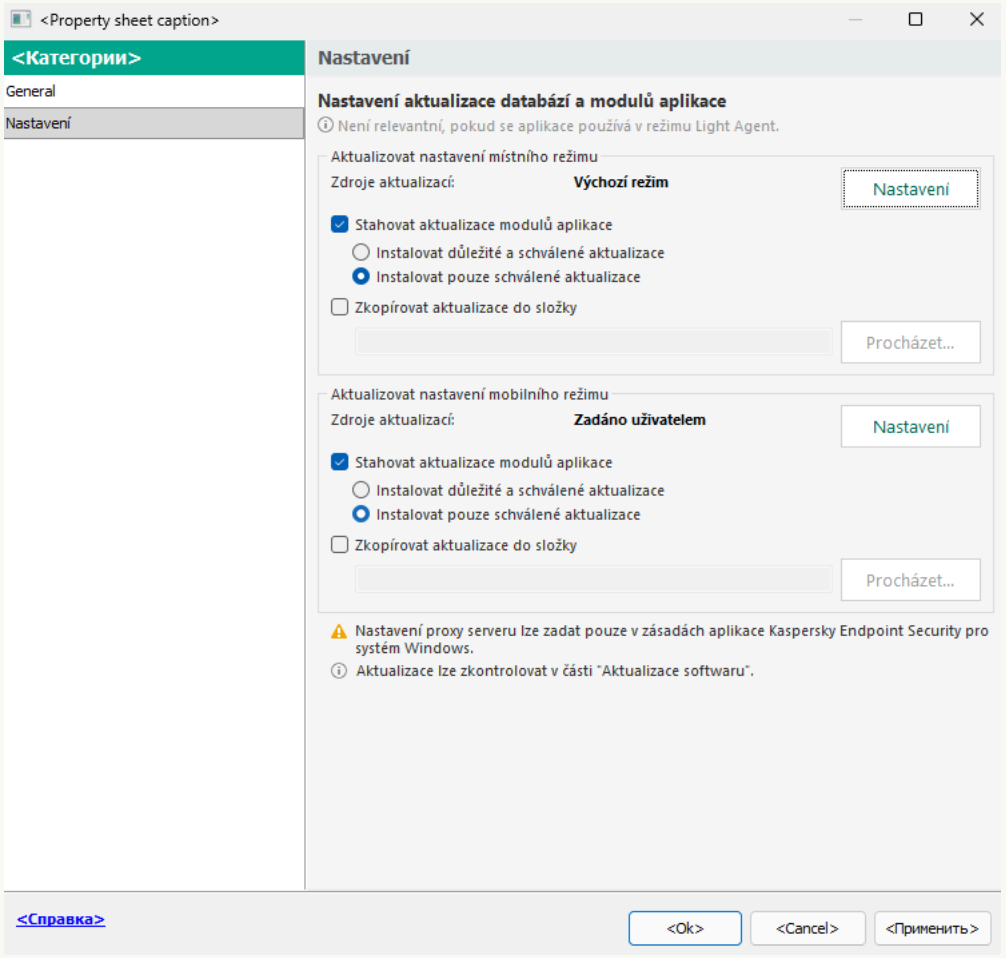
      Úlohu *Aktualizace databází a modulů aplikace* je nutné přiřadit k jednomu počítači, který bude sloužit jako zdroj aktualizací.

   3. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

      Otevře se okno vlastností úlohy.

      Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

   4. V okně vlastností úlohy vyberte část **Settings**.



Nastavení úlohy Aktualizace databází a modulů aplikace

   5. V bloku **Aktualizovat nastavení místního režimu** klikněte na tlačítko **Nastavení**.
   6. 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.

7. Zaškrtněte políčko **Zkopírovat aktualizace do složky**.
8. Do pole **Cesta ke složce** zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).

   Pokud je políčko ponecháno prázdné, aplikace Kaspersky Endpoint Security zkopíruje aktualizační balíček do složky `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.
9. Uložte změny.

[Jak povolit kopírování aktualizačního balíčku do sdílené složky ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

   > Úlohu *Update* je nutné přiřadit k jednomu počítači, který bude sloužit jako zdroj aktualizací.

2. Klikněte na úlohu **Update** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Update* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Update*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.
3. Vyberte kartu **Application settings** → **Local mode**.
4. Nakonfigurujte zdroje aktualizací.

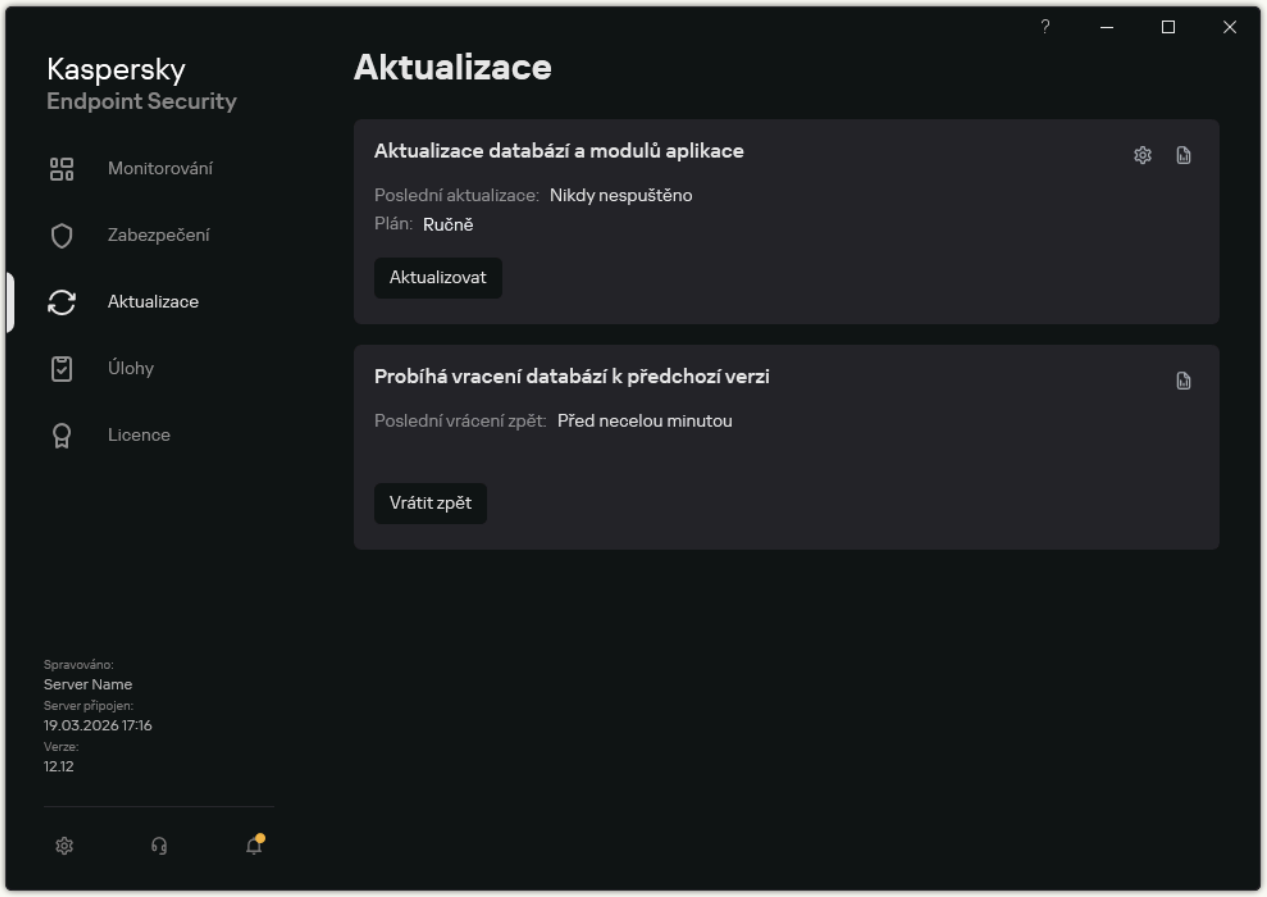
   Mezi zdroje aktualizací mohou patřit aktualizační servery společnosti Kaspersky, server pro správu aplikace Kaspersky Security Center, další servery FTP nebo HTTP, místní složky nebo síťové složky.
5. Zaškrtněte políčko **Copy updates to folder**.
6. Do pole **Path** zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).

   Pokud je políčko ponecháno prázdné, aplikace Kaspersky Endpoint Security zkopíruje aktualizační balíček do složky `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.
7. Uložte změny.

[Jak povolit kopírování aktualizačního balíčku do sdílené složky v rozhraní aplikace]

> Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.
   Otevře se okno vlastností úlohy.
3. V bloku **Distribuce aktualizací** zaškrtněte políčko **Zkopírovat aktualizace do složky**.
4. Zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).
5. Uložte změny.

3. Konfigurace aktualizací databází a modulů aplikace z určené sdílené složky do zbývajících počítačů v síti LAN organizace.
   Jak konfigurovat aktualizace ze sdílené složky v konzole pro správu (MMC)

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Aktualizace databází a modulů aplikace**.
4. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
5. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Aktualizace databází a modulů aplikace**.

Krok 2. Výběr zdrojů aktualizací

Přidejte nový zdroj aktualizací: sdílenou složku. Zdrojová adresa se musí shodovat s adresou, kterou jste dříve zadali v poli **Cesta ke složce** při konfiguraci kopírování balíčku aktualizace do sdílené složky. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

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.

Úlohu *Aktualizace databází a modulů aplikace* je nutné přiřadit k počítačům v síti LAN organizace, kromě počítače, který slouží jako zdroj aktualizací.

Krok 4. Výběr účtu pro spuštění úlohy

Vyberte účet pro spuštění úlohy *Aktualizace databází a modulů aplikace*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.

Krok 5. Konfigurace plánu spuštění úlohy

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

Krok 6. Definování názvu úlohy

Zadejte název úlohy, například *Aktualizace ze sdílené složky*.

Krok 7. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. V důsledku toho bude úloha aktualizace provedena v počítačích uživatelů podle určeného plánu.

Jak nakonfigurovat aktualizace ze sdílené složky ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Update**.
   c. Do pole **Task name** zadejte krátký popis, například *Aktualizace ze sdílené složky*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

   Úlohu *Update* 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 přejděte k dalšímu kroku.
5. Ukončete průvodce.
   V tabulce úloh se zobrazí nová úloha.

6. Klikněte na nově vytvořenou úlohu *Update*.

   Otevře se okno vlastností úlohy.

7. Vyberte kartu **Application settings** → **Local mode**.

8. V bloku **Update sources** klikněte na tlačítko **Add**.

9. V okně, které se otevře, zadejte cestu ke sdílené složce.

   Zdrojová adresa se musí shodovat s adresou, kterou jste dříve zadali v poli **Path** při konfiguraci kopírování balíčku aktualizace do sdílené složky (viz výše uvedené pokyny).

10. Klikněte na tlačítko **OK**.

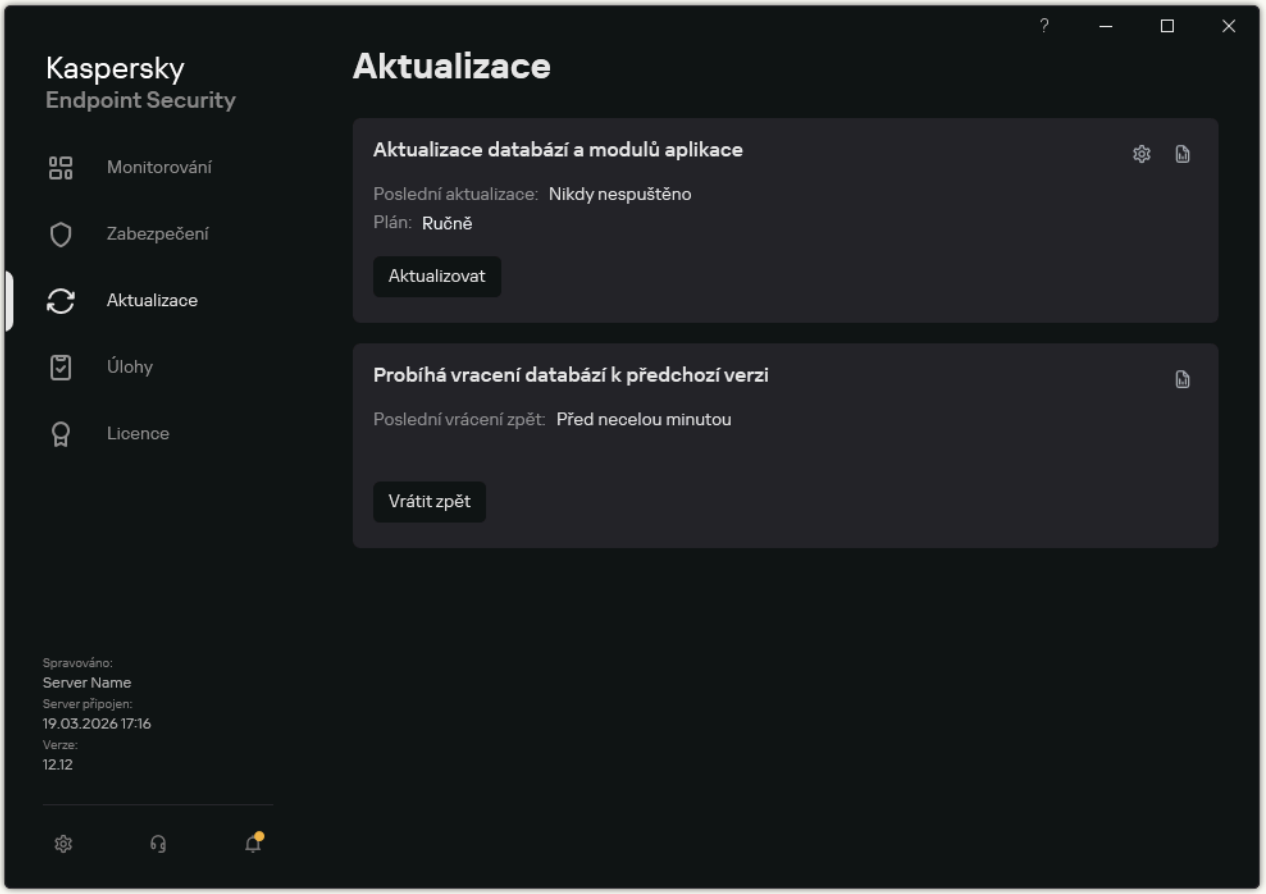
11. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Up** a **Down**.

12. Uložte změny.

Jak nakonfigurovat aktualizace ze sdílené složky v rozhraní aplikace

Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.

   Otevře se okno vlastností úlohy.

3. Klikněte na tlačítko **Vybrat zdroje aktualizací**.

4. V okně, které se otevře, klikněte na tlačítko **Přidat**.

5. V okně, které se otevře, zadejte cestu ke sdílené složce.

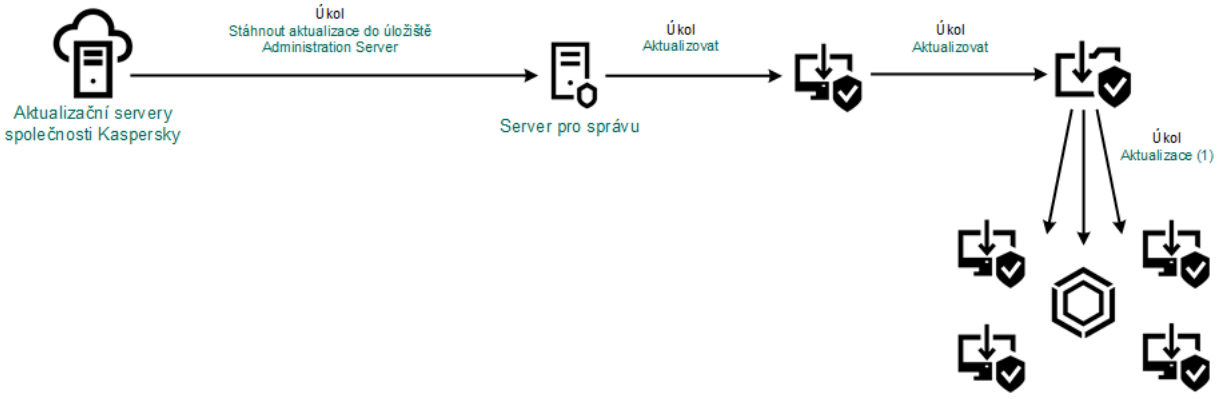
   Zdrojová adresa se musí shodovat s adresou, kterou jste dříve zadali při konfiguraci kopírování balíčku aktualizace do sdílené složky (viz výše uvedené pokyny).

6. Klikněte na tlačítko **Vybrat**.

7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

8. Uložte změny.



Aktualizace ze sdílené složky

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.

Verze a lokalizace aplikace Kaspersky Endpoint Security, která zkopíruje aktualizační balíček do sdílené složky, musí odpovídat verzi a lokalizaci aplikace, která aktualizuje databáze ze sdílené složky. Pokud se verze nebo lokalizace aplikací neshodují, může aktualizace databáze skončit chybou.

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.

   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.

4. Konfigurace aktualizací databází a modulů aplikace z určené sdílené složky do zbývajících počítačů v síti LAN organizace.

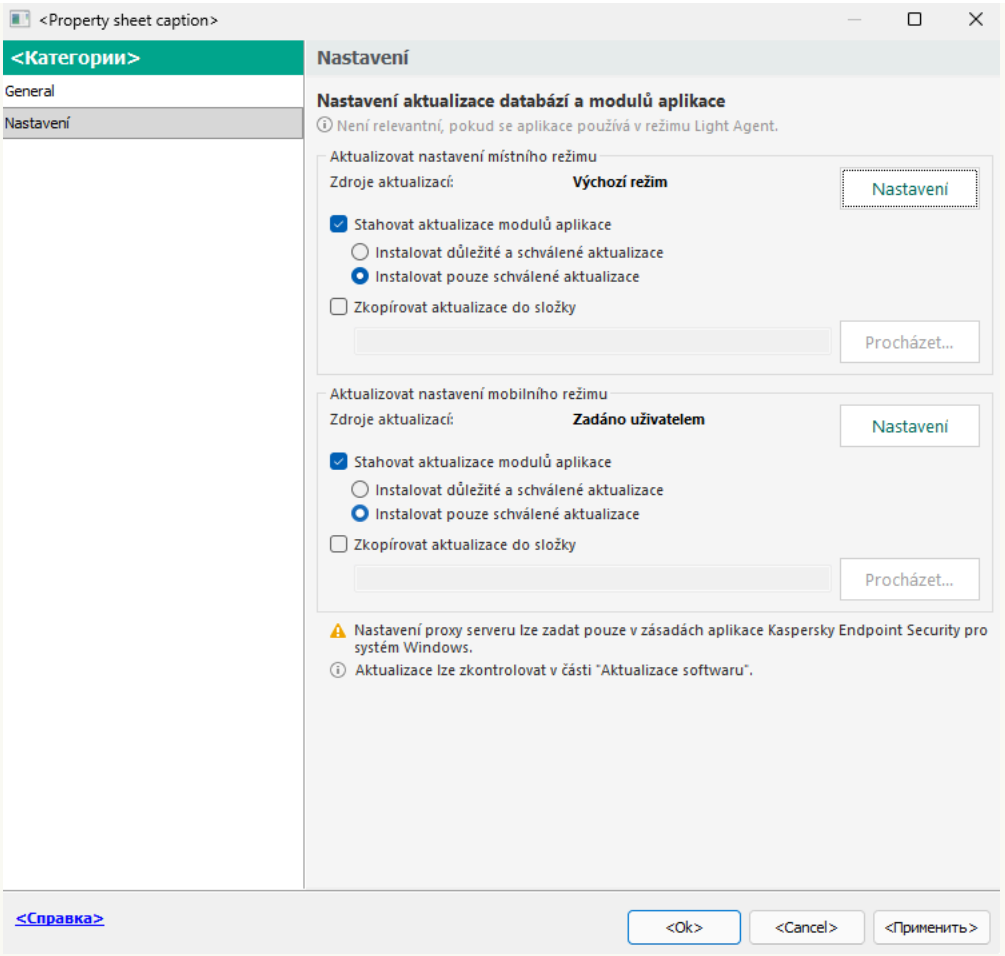
   Jak konfigurovat aktualizace ze sdílené složky v konzole pro správu (MMC)

   1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
   2. Ve stromu konzoly vyberte možnost **Tasks**.
   3. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

      Otevře se okno vlastností úlohy.

      Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

   4. V okně vlastností úlohy vyberte část **Settings**.



Nastavení úlohy Aktualizace databází a modulů aplikace

5. V bloku **Aktualizovat nastavení místního režimu** klikněte na tlačítko **Nastavení**.
6. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.
7. V okně, které se otevře, zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).

   Zdrojová adresa se musí shodovat s adresou uvedenou v nastavení nástroje Kaspersky Update Utility.

8. Klikněte na tlačítko **OK**.
9. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

10. Uložte změny.

[Jak nakonfigurovat aktualizace ze sdílené složky ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Update** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Update* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Update*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Application settings** → **Local mode**.
4. V seznamu zdrojů aktualizací klikněte na tlačítko **Add**.
5. V okně, které se otevře, zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).

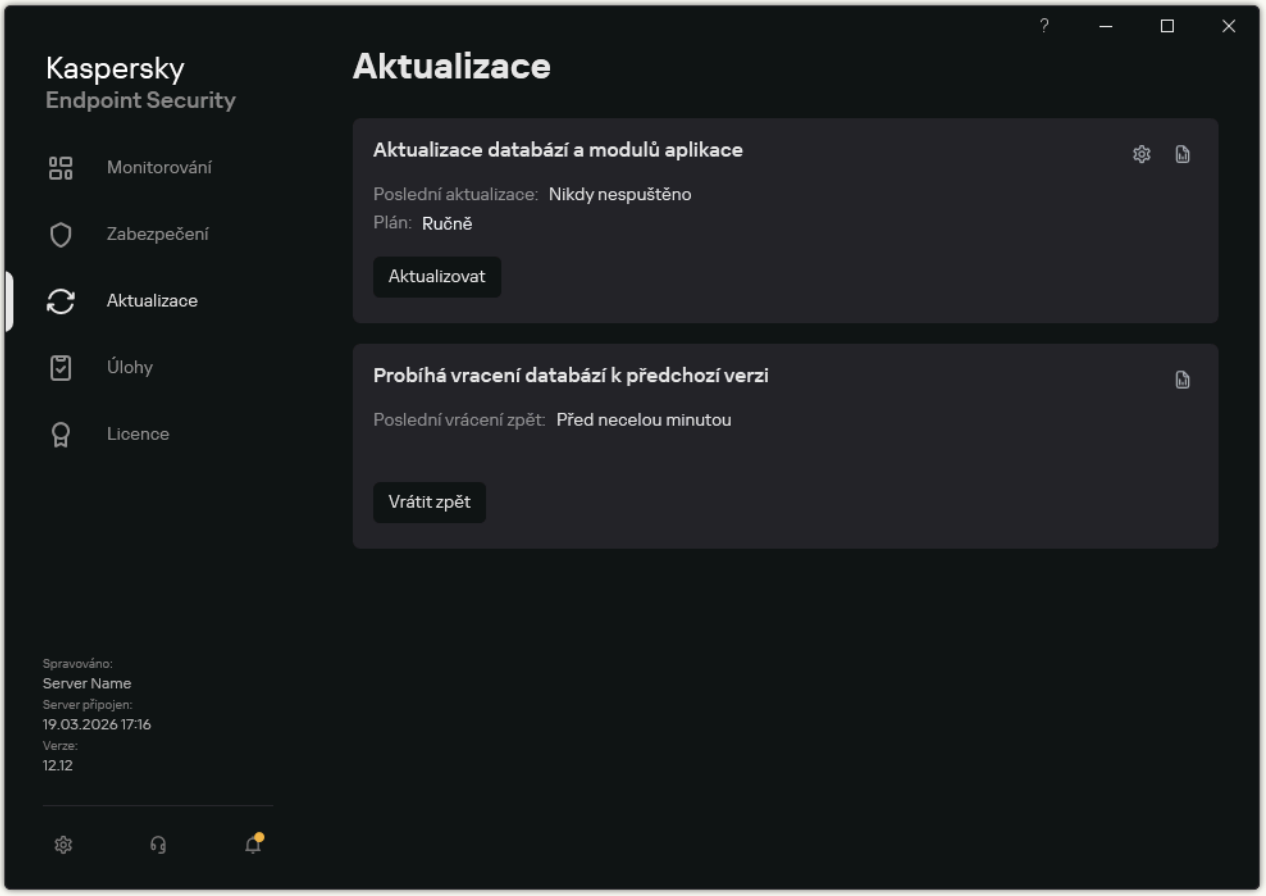
Zdrojová adresa se musí shodovat s adresou uvedenou v nastavení nástroje Kaspersky Update Utility.

6. Klikněte na tlačítko **OK**.
7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.
   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.
8. Uložte změny.

[Jak nakonfigurovat aktualizace ze sdílené složky v rozhraní aplikace](#)

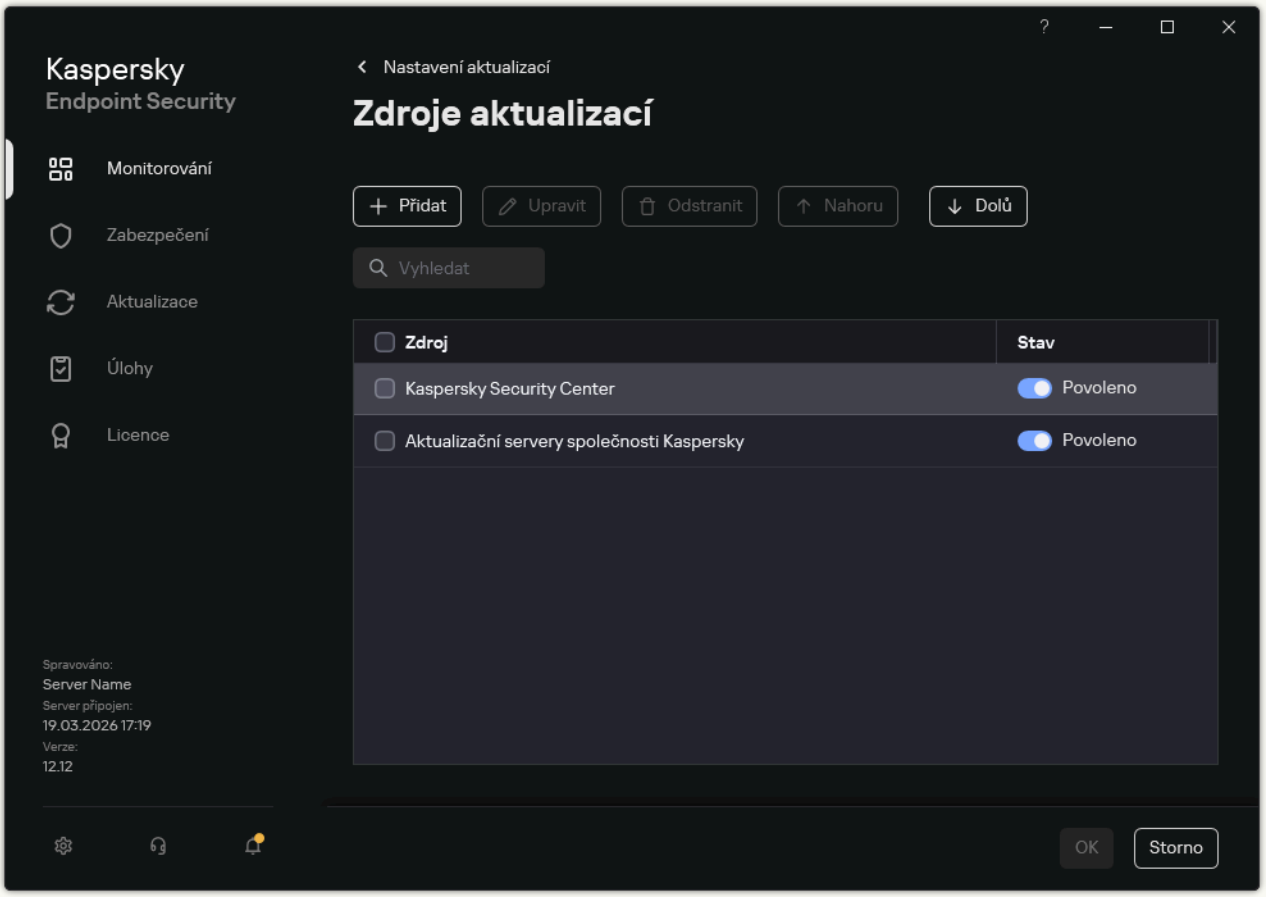
Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.
   Otevře se okno vlastností úlohy.
3. V okně vlastností úlohy klikněte na možnost **Vybrat zdroje aktualizací**.
4. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.



Zdroje aktualizace

5. Zadejte cestu UNC ke sdílené složce (například `\\<server name>\KLSHARE\Updates`).

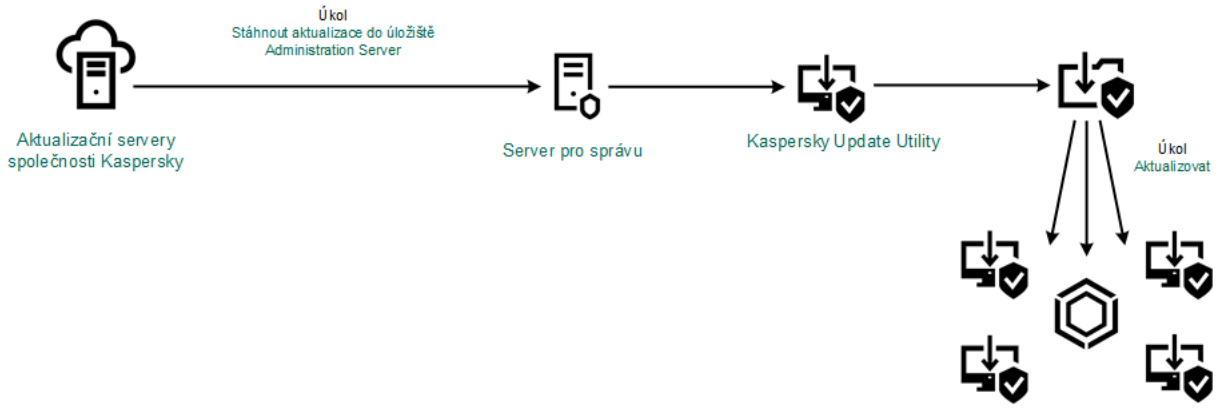
   Zdrojová adresa se musí shodovat s adresou uvedenou v nastavení nástroje Kaspersky Update Utility.

6. Klikněte na tlačítko **Vybrat**.

7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.

8. Uložte změny.



Aktualizace pomocí nástroje Kaspersky Update Utility

Aktualizace v mobilním režimu

Mobile mode 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.

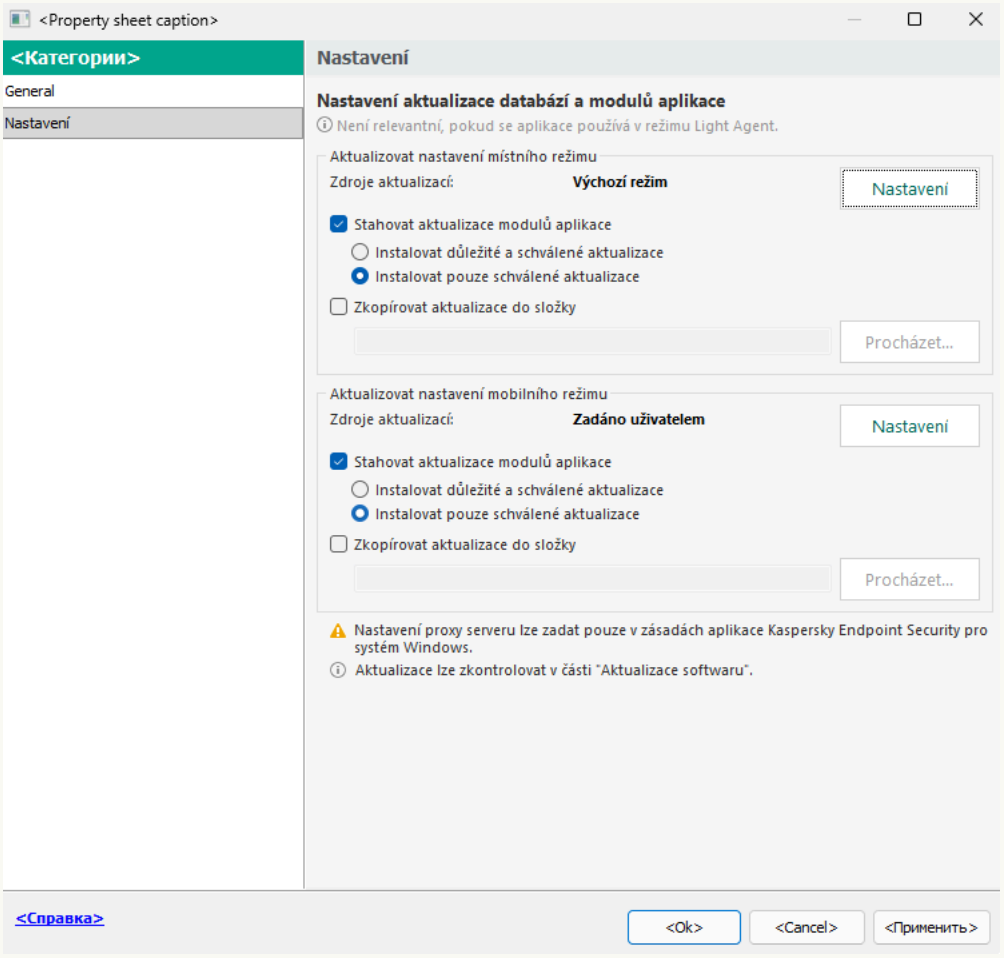
Počítač v režimu offline mimo síť organizace se nemůže připojit k serveru pro správu, aby aktualizoval databáze a moduly aplikace. Ve výchozím nastavení jsou jako zdroj aktualizace pro aktualizaci databází a modulů aplikací v mobilním režimu použity pouze aktualizační servery společnosti Kaspersky. Použití 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.

Jak nakonfigurovat aktualizaci nastavení mobilního režimu v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.
4. V okně vlastností úlohy vyberte část **Settings**.



Nastavení úlohy Aktualizace databází a modulů aplikace

5. V bloku **Aktualizovat nastavení mobilního režimu** klikněte na tlačítko **Nastavení**.
6. Nakonfigurujte zdroje aktualizací. Mezi zdroje aktualizací mohou patřit aktualizační servery společnosti Kaspersky, další servery FTP a HTTP, místní složky nebo síťové složky.
7. Uložte změny.

Jak nakonfigurovat aktualizaci nastavení mobilního režimu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Update** Kaspersky Endpoint Security.

Otevře se okno vlastností úlohy.

Úloha *Update* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Update*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Application settings** → **Mobile mode**.

4. Nakonfigurujte zdroje aktualizací. Mezi zdroje aktualizací mohou patřit aktualizační servery společnosti Kaspersky, další servery FTP a HTTP, místní složky nebo síťové složky.

5. Uložte změny.

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 přejděte do části **Aktualizace**.

2. Chcete-li spustit úlohu aktualizace, na dlaždici **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. Úlohu můžete kdykoli zastavit kliknutím na tlačítko **Zastavit aktualizaci**.

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.

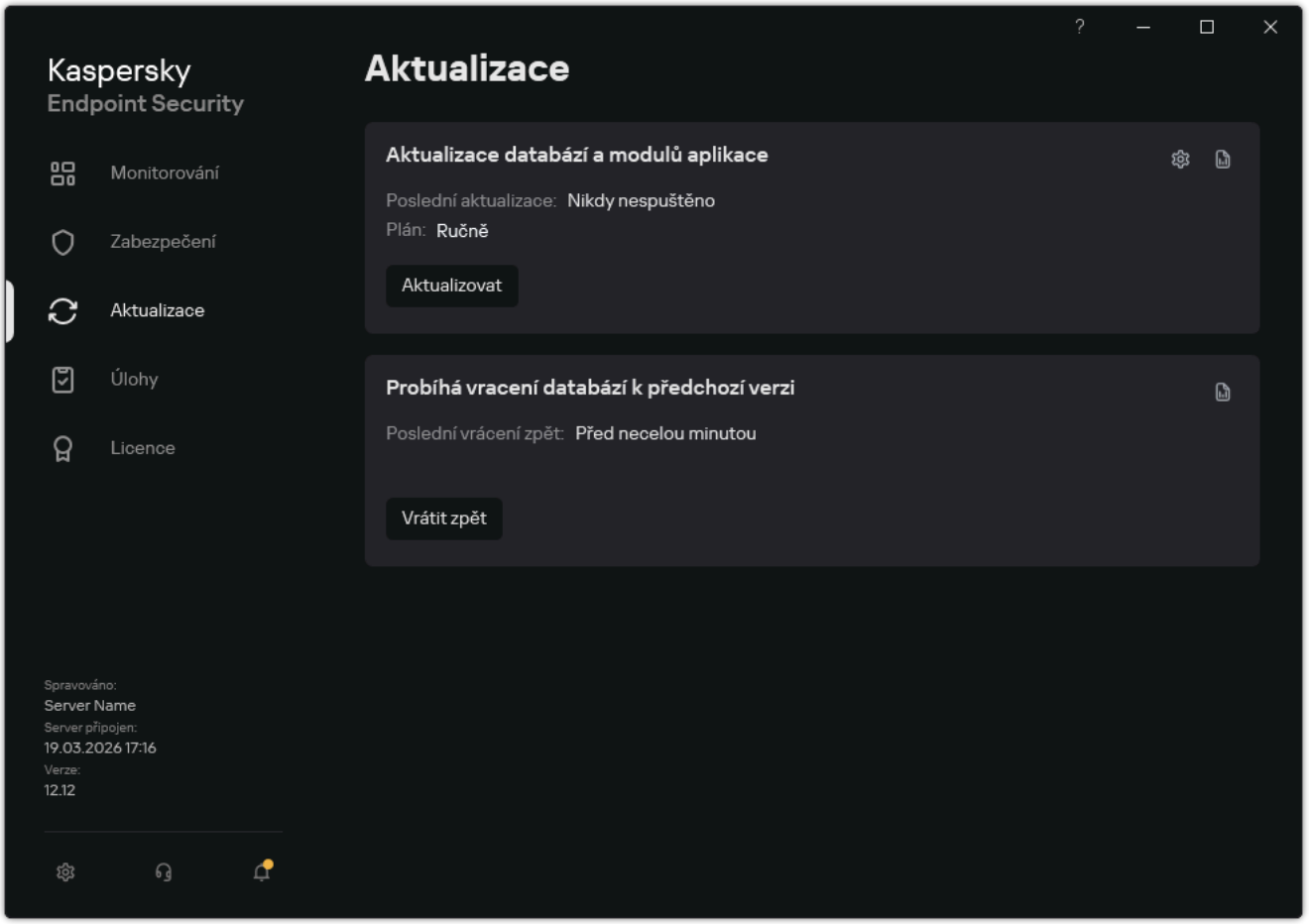
Spuštění úlohy aktualizace za použití oprávnění jiného uživatelského účtu

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 aplikace 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:

Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.

   Otevře se okno vlastností úlohy.

3. Klikněte na tlačítko **Spustit aktualizace databází s uživatelskými oprávněními**.

4. V okně, které se otevře, vyberte **Jiný uživatel**.

5. Zadejte přihlašovací údaje k účtu uživatele s potřebnými oprávněními pro přístup ke zdroji aktualizace.

6. Uložte změny.

Volba režimu spuštění úlohy aktualizace

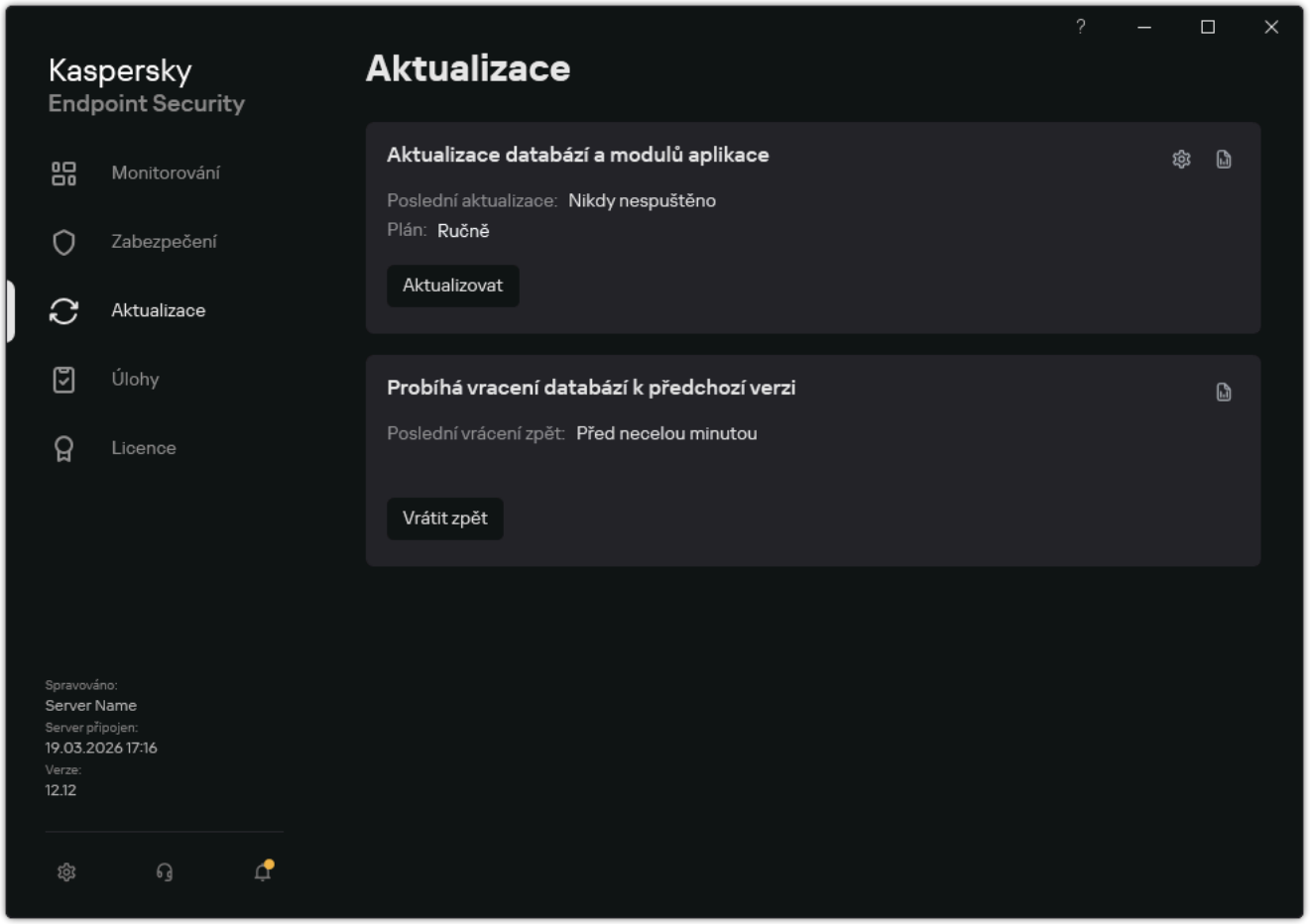
Pokud z jakéhokoli důvodu nelze úlohu aktualizace spustit (například, když je počítač vypnutý), můžete nakonfigurovat automatické spuštění vynechané úlohy ihned, jakmile to bude možné.

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:

Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.

   Otevře se okno vlastností úlohy.

3. Klikněte na tlačítko **Režim spouštění**.

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 jiné možnosti. Konfigurace rozšířeného nastavení pro spuštění úlohy aktualizace:
     - Do pole **Odložit spuštění úlohy po startu aplikace o N minut** zadejte časový interval pro spuštění úlohy aktualizace poté, co se spustí aplikace Kaspersky Endpoint Security.
     - Jestliže chcete, aby aplikace Kaspersky Endpoint Security při první příležitosti spustila zmeškané úlohy aktualizace, vyberte možnost **Spustit plánovanou kontrolu následující den, pokud bude počítač vypnutý**. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače.

5. Uložte změny.

Přidání zdroje aktualizací

Aktualizační zdroj 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.

Pokud nejsou aktualizační servery Kaspersky dostupné, Kaspersky Endpoint Security může k aktualizaci databází a modulů aplikačního softwaru použít alternativní domény. Podrobné informace naleznete ve znalostní bázi technické podpory.

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.

Ve výchozím nastavení používá Kaspersky Endpoint Security jako první zdroj aktualizací server Kaspersky Security Center. To pomáhá šetřit provoz při aktualizaci. Pokud na počítač nejsou aplikovány zásady, jako první zdroj aktualizací jsou v nastavení místní úlohy *Aktualizace databází a modulů aplikace* vybrány servery společnosti Kaspersky, protože aplikace nemusí mít přístup k serveru Kaspersky Security Center.

Pokud je aplikace spuštěna v režimu Light Agent, jako aktualizační zdroj je vybrána složka na SVM.

Jak přidat zdroj aktualizace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

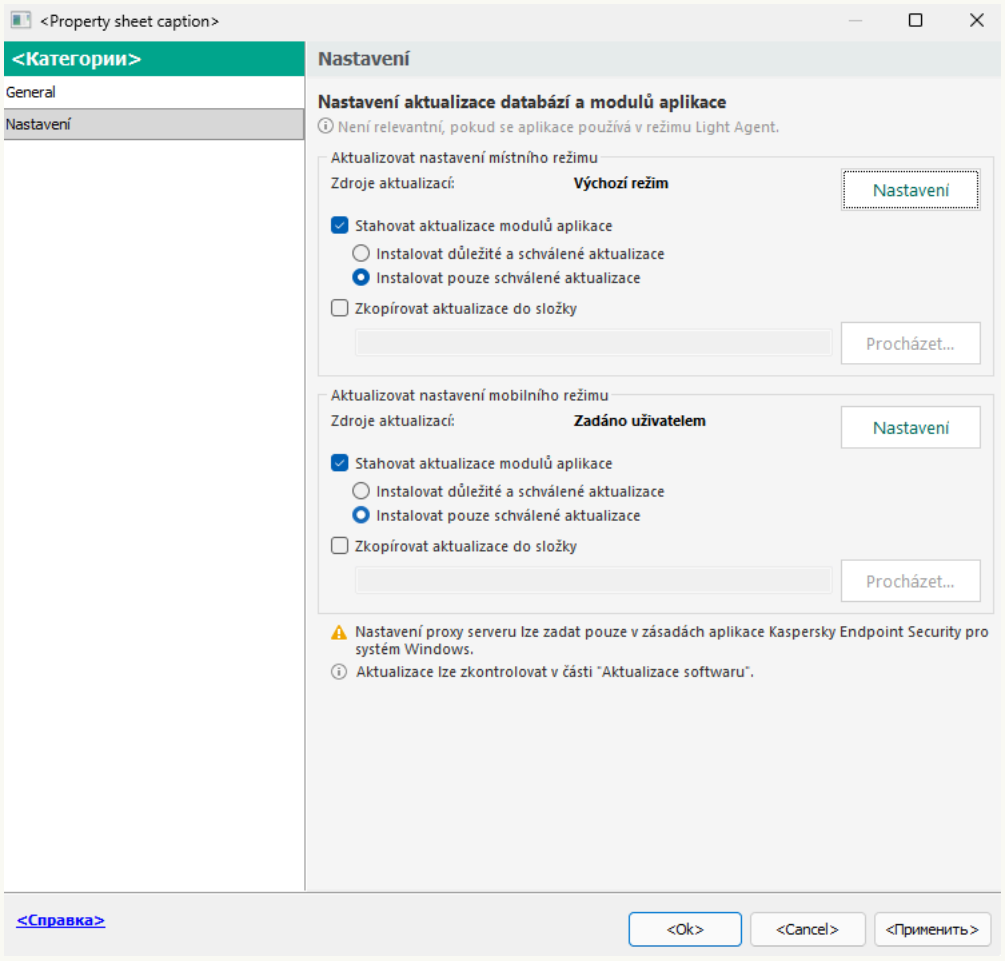
   Ve stromu konzoly vyberte možnost **Tasks**.

2. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

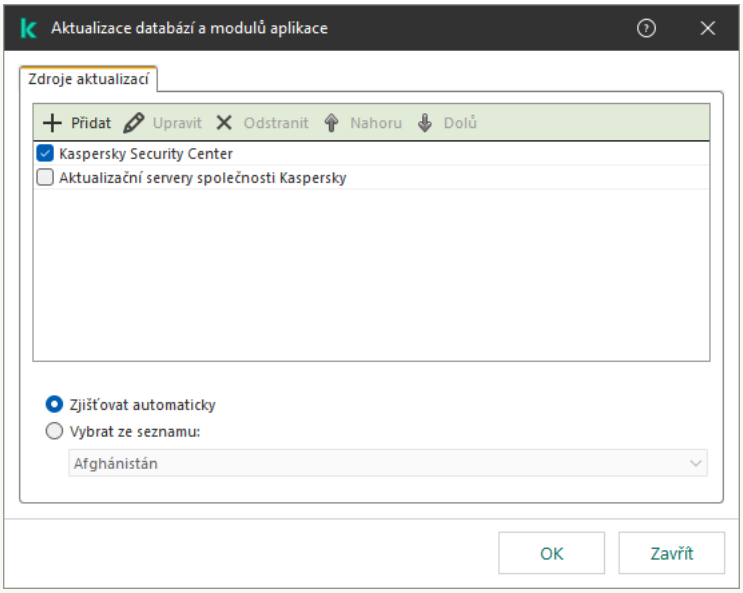
   Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

3. V okně vlastností úlohy vyberte část **Nastavení**.



Nastavení úlohy Aktualizace databází a modulů aplikace

4. V bloku **Aktualizovat nastavení místního režimu** klikněte na tlačítko **Nastavení**.



Zdroje aktualizace

5. V seznamu zdrojů aktualizací klikněte na tlačítko **Přidat**.
6. Do pole **Zdroje aktualizací** 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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

   Zdroj aktualizací můžete vyloučit, aniž byste jej odebírali ze seznamu zdrojů aktualizací. Chcete-li tak učinit, zrušte zaškrtnutí políčka vedle objektu.
7. Klikněte na tlačítko **OK**.
8. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Nahoru** a **Dolů**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.
9. V případě potřeby přidejte zdroj aktualizací pro mobilní režim. *Mobile mode* je režim fungování aplikace Kaspersky Endpoint Security, kdy počítač opustí hranice sítě organizace (*počítač v režimu offline*).
10. Uložte změny.

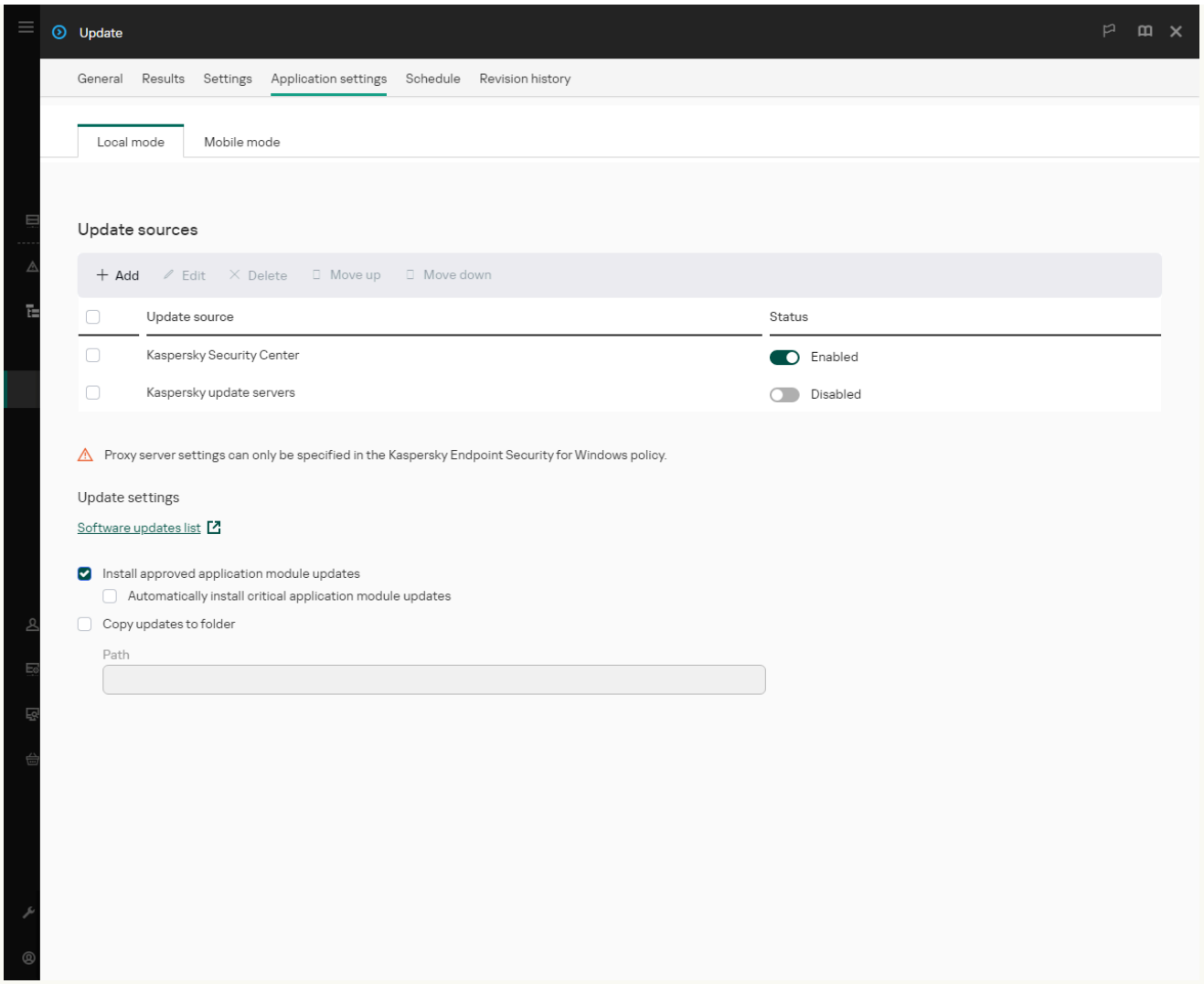
Jak přidat zdroj aktualizací ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Update** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Update* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Update*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.
3. Vyberte kartu **Application settings** → **Local mode**.



Zdroje aktualizace

4. V seznamu zdrojů aktualizací klikněte na tlačítko **Add**.
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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

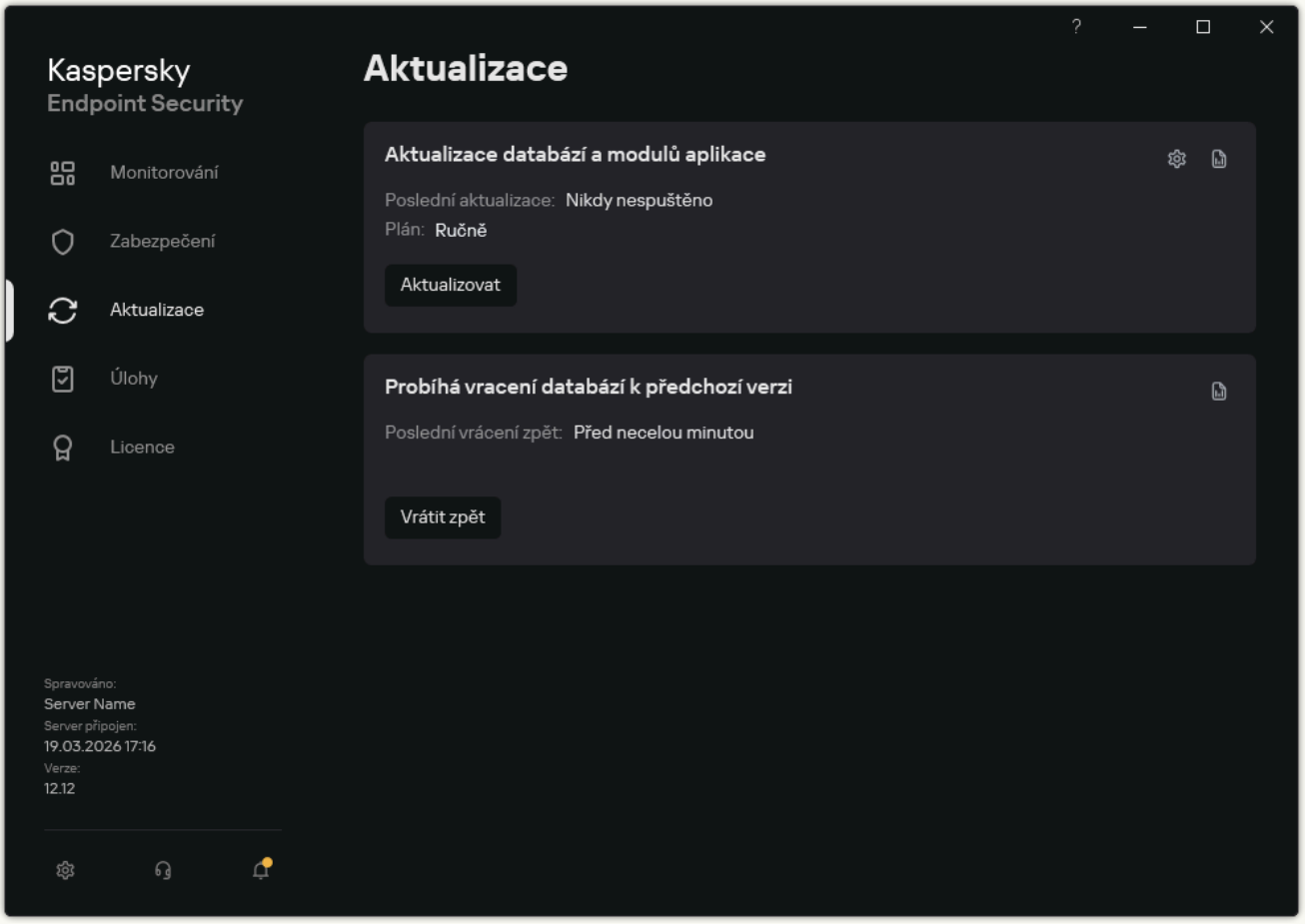
   Zdroj aktualizací můžete vyloučit, aniž byste jej odebírali ze seznamu zdrojů aktualizací. Chcete-li to provést, přepněte přepínač vedle něj do polohy vypnuto.
6. Klikněte na tlačítko **OK**.
7. Nakonfigurujte priority zdrojů aktualizací pomocí tlačítek **Up** a **Down**.

   Pokud nelze provést aktualizaci z prvního aktualizačního zdroje, aplikace Kaspersky Endpoint Security automaticky přejde na další zdroj.
8. V případě potřeby přidejte zdroj aktualizací pro mobilní režim. *Mobile mode* je režim fungování aplikace Kaspersky Endpoint Security, kdy počítač opustí hranice sítě organizace (*počítač v režimu offline*).
9. Uložte změny.

Jak přidat zdroj aktualizací v rozhraní aplikace

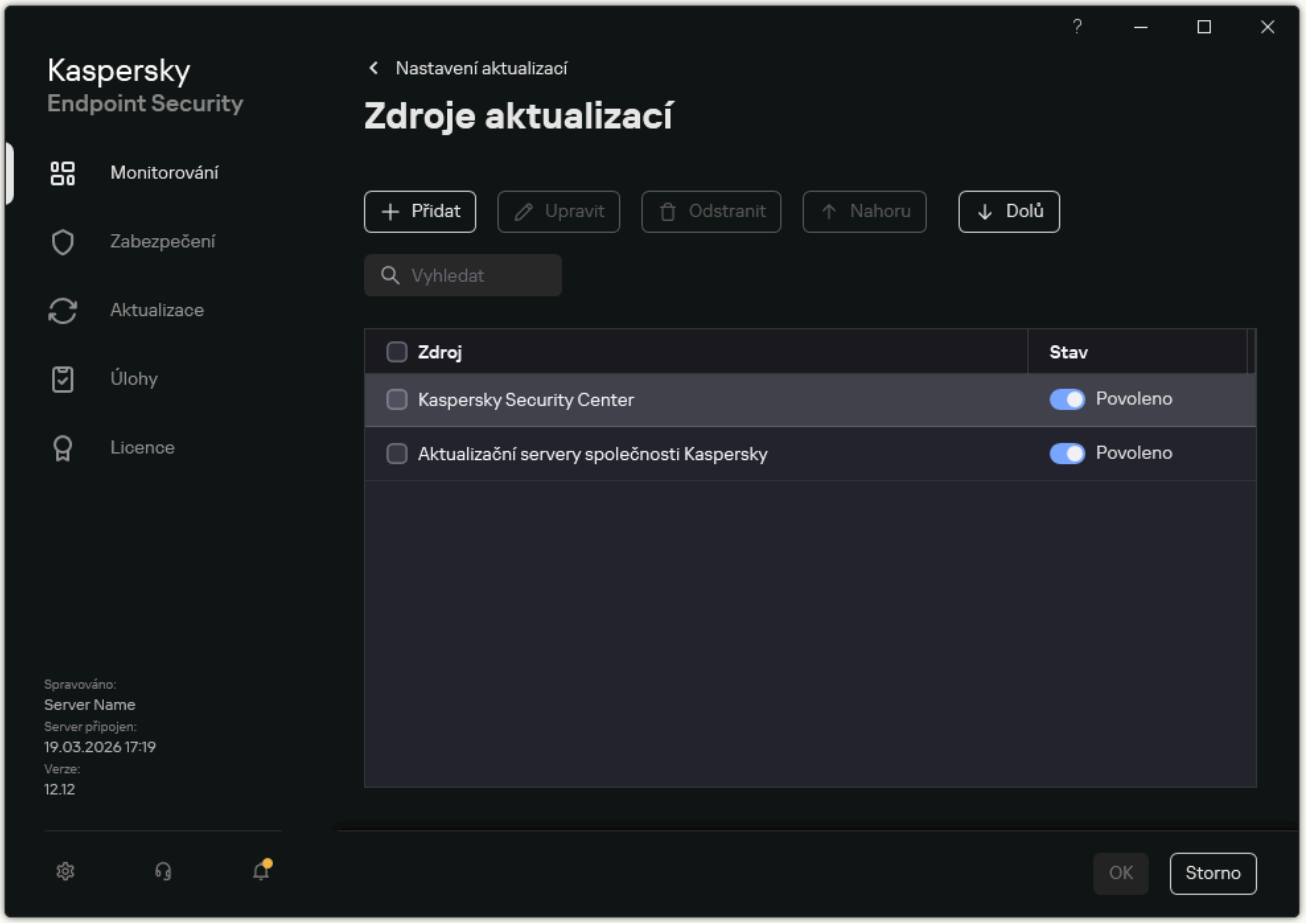
Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.
   Otevře se okno vlastností úlohy.
3. Klikněte na tlačítko **Vybrat zdroje aktualizací**.
4. V okně, které se otevře, klikněte na tlačítko **Přidat**.



Zdroje aktualizace

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://<user name>:<password>@<node>:<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\AVP12\Update distribution\`.

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. Kdykoli je k dispozici aktualizace, aplikace zobrazí v hlavním okně aplikace Kaspersky Endpoint Security oznámení. 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.

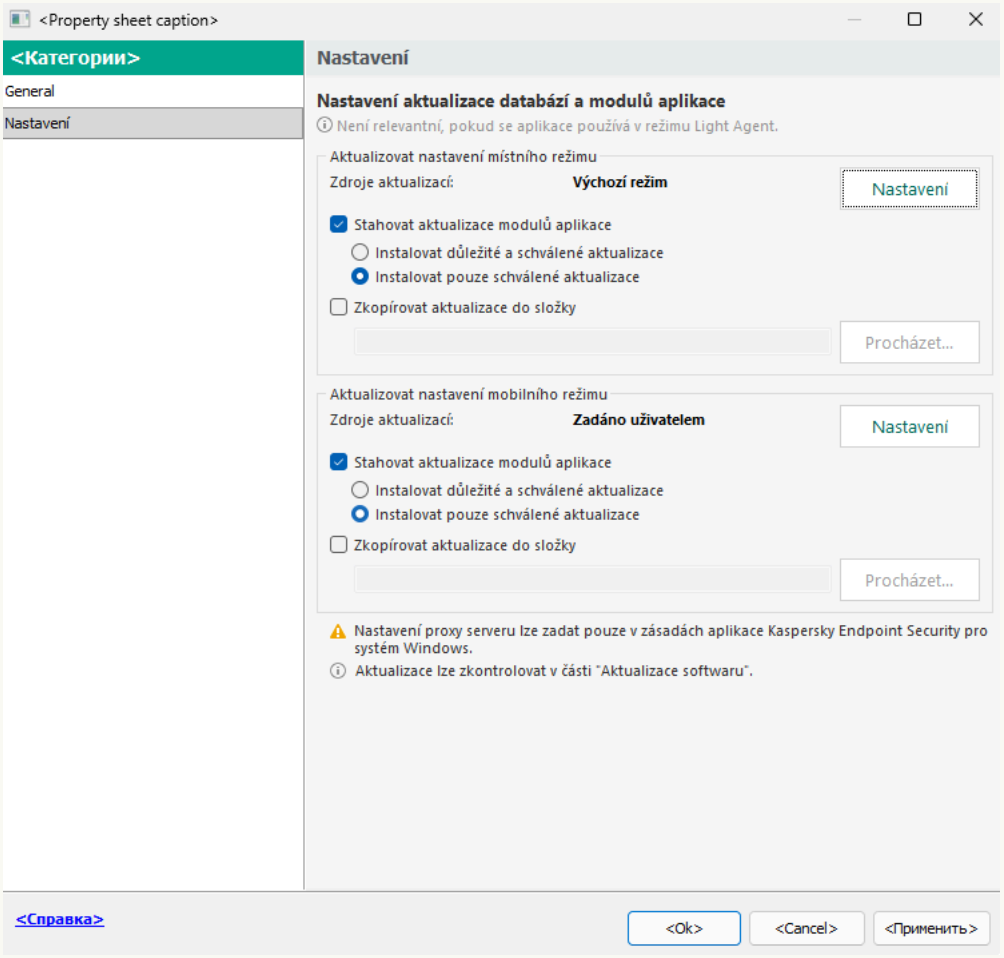
Po instalaci aktualizace aplikace může být nutné restartovat počítač.

Jak konfigurovat aktualizace modulu aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.
4. V okně vlastností úlohy vyberte část **Settings**.



Nastavení úlohy Aktualizace databází a modulů aplikace

5. V bloku **Aktualizovat nastavení místního režimu** zaškrtněte políčko **Stahovat aktualizace modulů aplikace**.

   Pokud chcete zabránit stahování aktualizací modulu aplikace, zrušte zaškrtnutí políčka **Stahovat aktualizace modulů aplikace** a zakažte používání místních úloh uživatelem.
6. 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.
7. Pokud je potřeba, nakonfigurujte aktualizace modulu aplikace pro mobilní režim. *Mobile mode* je režim fungování aplikace Kaspersky Endpoint Security, kdy počítač opustí hranice sítě organizace (*počítač v režimu offline*).
8. Uložte změny.

Jak konfigurovat aktualizace modulu aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

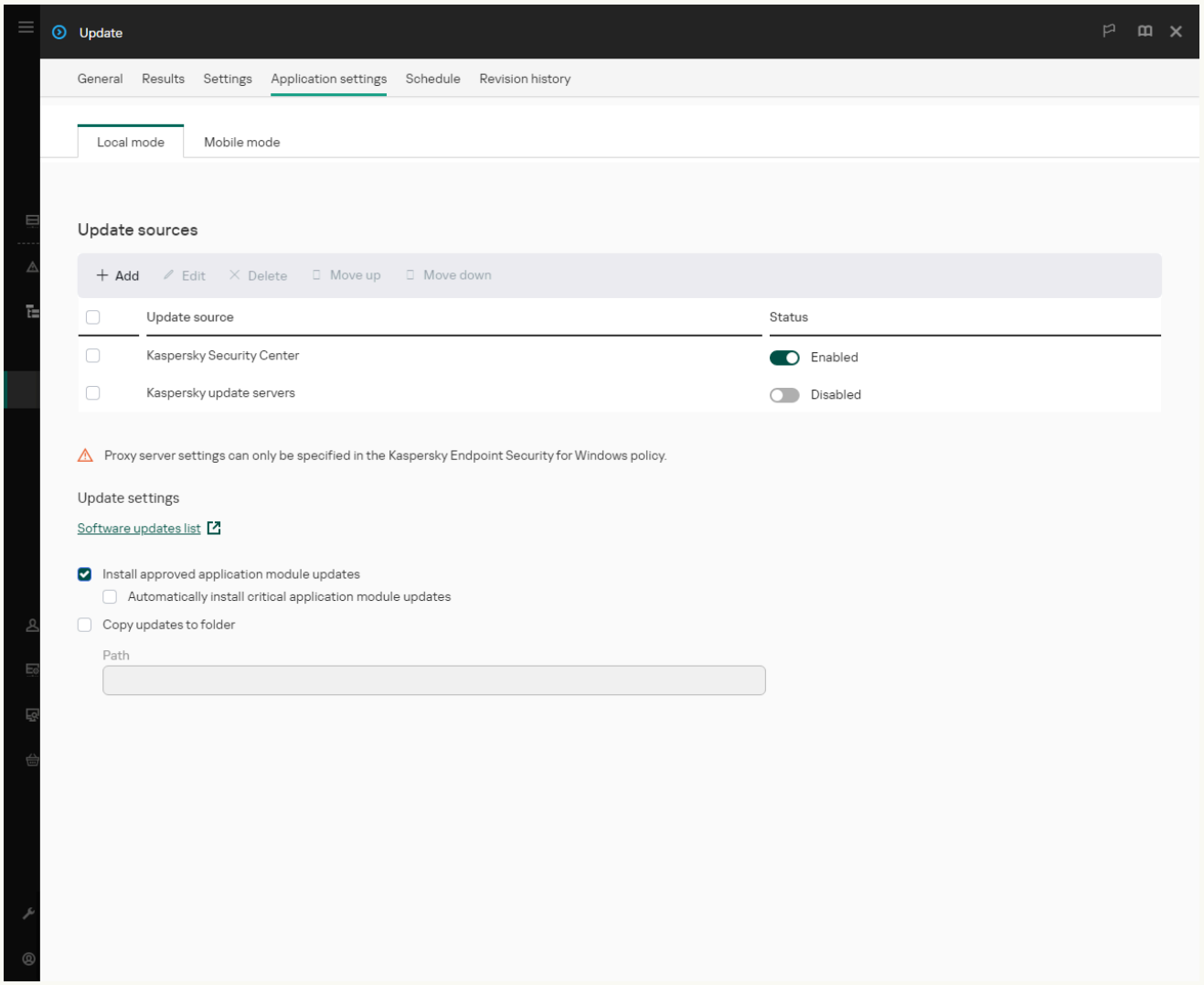
   Otevře se seznam úloh.

2. Klikněte na úlohu **Aktualizace databází a modulů aplikace** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

   Úloha *Aktualizace databází a modulů aplikace* je vytvořena automaticky průvodcem rychlým spuštěním serveru pro správu. Chcete-li vytvořit úlohu *Aktualizace databází a modulů aplikace*, nainstalujte při spuštění průvodce modul plug-in administrace aplikace Kaspersky Endpoint Security pro systém Windows.

3. Vyberte kartu **Application settings** → **Local mode**.



Nastavení úlohy Update

4. V části **Update settings** vyberte aktualizace modulu aplikace, které chcete nainstalovat:

   - **Install approved application module updates**. 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.

   - **Automatically install critical application module updates**. 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.

   Pokud chcete zabránit stahování aktualizací modulu aplikace, zrušte zaškrtnutí políček **Install approved application module updates** a **Automatically install critical application module updates** a zakažte používání místních úloh uživatelem.

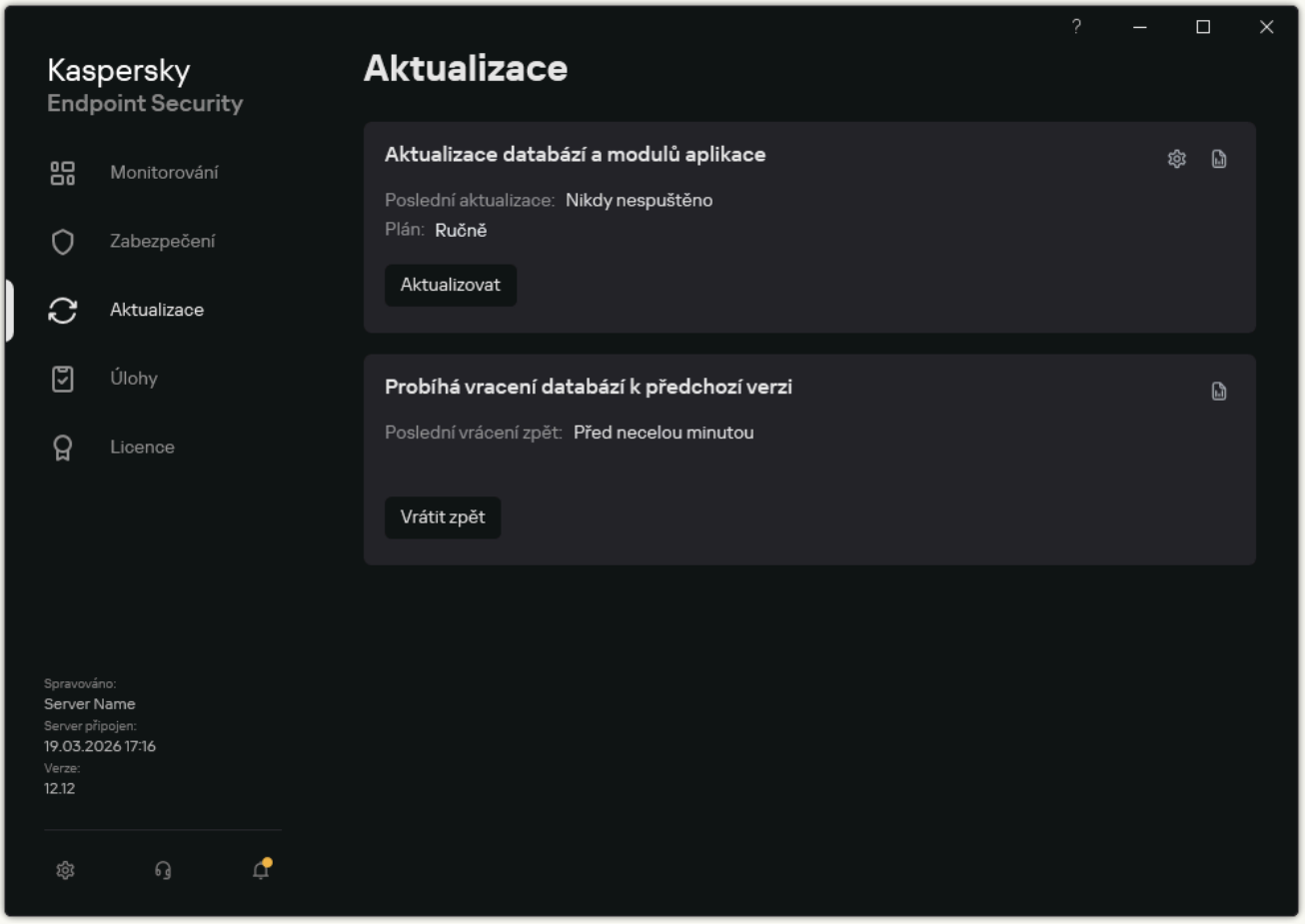
5. Pokud je potřeba, nakonfigurujte aktualizace modulu aplikace pro mobilní režim. *Mobile mode* je režim fungování aplikace Kaspersky Endpoint Security, kdy počítač opustí hranice sítě organizace (*počítač v režimu offline*).

6. Uložte změny.

Jak konfigurovat aktualizace modulu aplikace v rozhraní aplikace

Úlohu skupiny *Aktualizace databází a modulů aplikace* nemůžete konfigurovat v rozhraní aplikace. Uživateli je k dispozici pouze úloha místní aktualizace, *Aktualizace databází a modulů aplikace*. Pokud se úloha *Aktualizace databází a modulů aplikace* nezobrazí, znamená to, že správce zakázal v zásadách používat místní úlohy.

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Otevře se seznam úloh; vyberte úlohu *Aktualizace databází a modulů aplikace* a klikněte na ⚙.

   Otevře se okno vlastností úlohy.

3. V bloku **Stahování a instalace aktualizací modulů aplikací** zaškrtněte políčko **Stahovat 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 konzoly klikněte na ikonu ⚙.

   Otevře se okno vlastností administračního serveru.

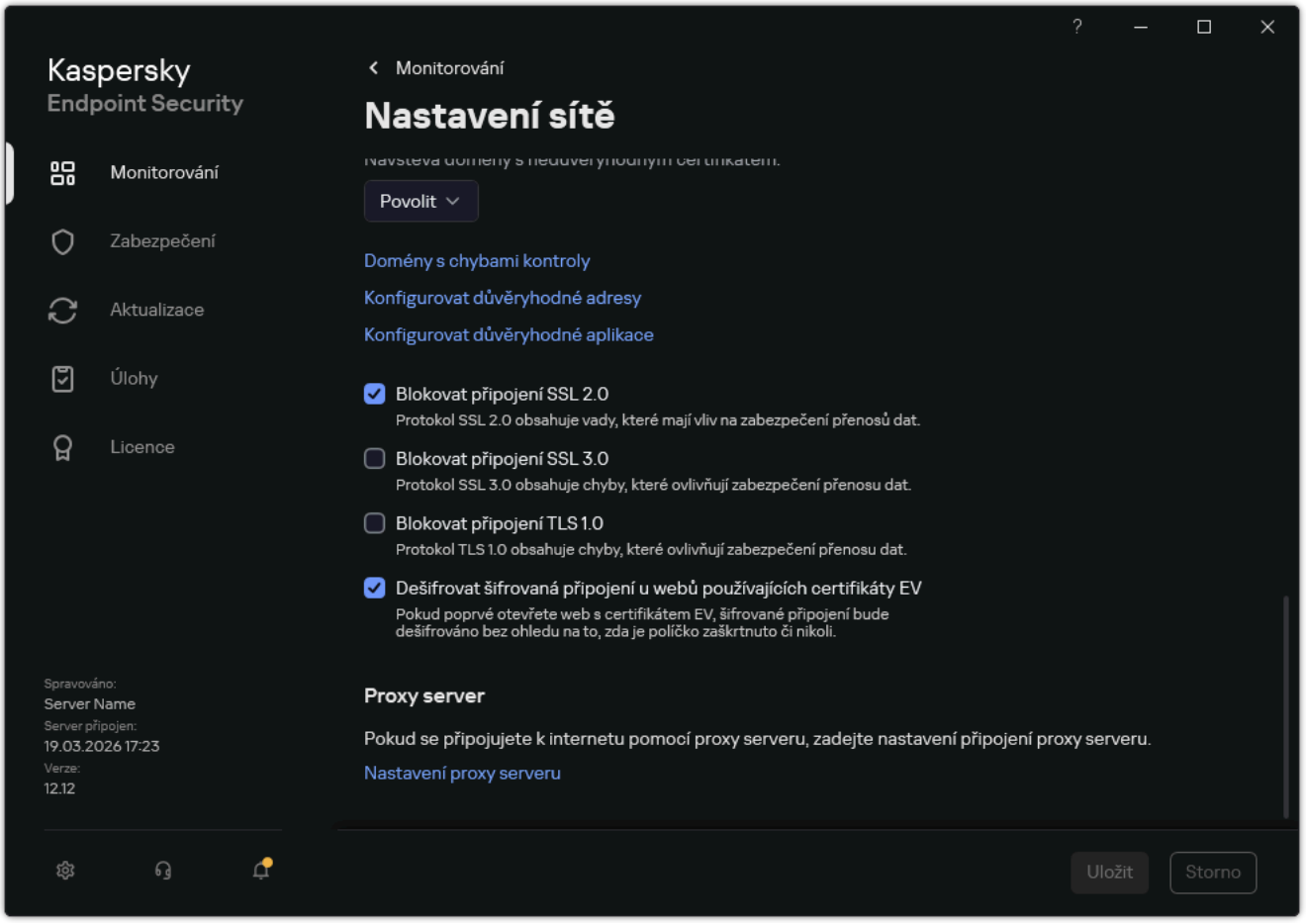
2. Přejděte do části **Configuring internet access**.
3. Zaškrtněte políčko **Use proxy server**.
4. Nakonfigurujte nastavení připojení proxy serveru: adresa proxy serveru, port a nastavení ověřování (uživatelské jméno a heslo).
5. Uložte změny.

Postup zakázání použití proxy serveru pro konkrétní skupinu pro správu:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. V bloku **Proxy server** klikněte na tlačítko **Settings**.
6. V okně, které se otevře, zaškrtněte políčko **Bypass a proxy server for local addresses**.
7. Uložte změny.

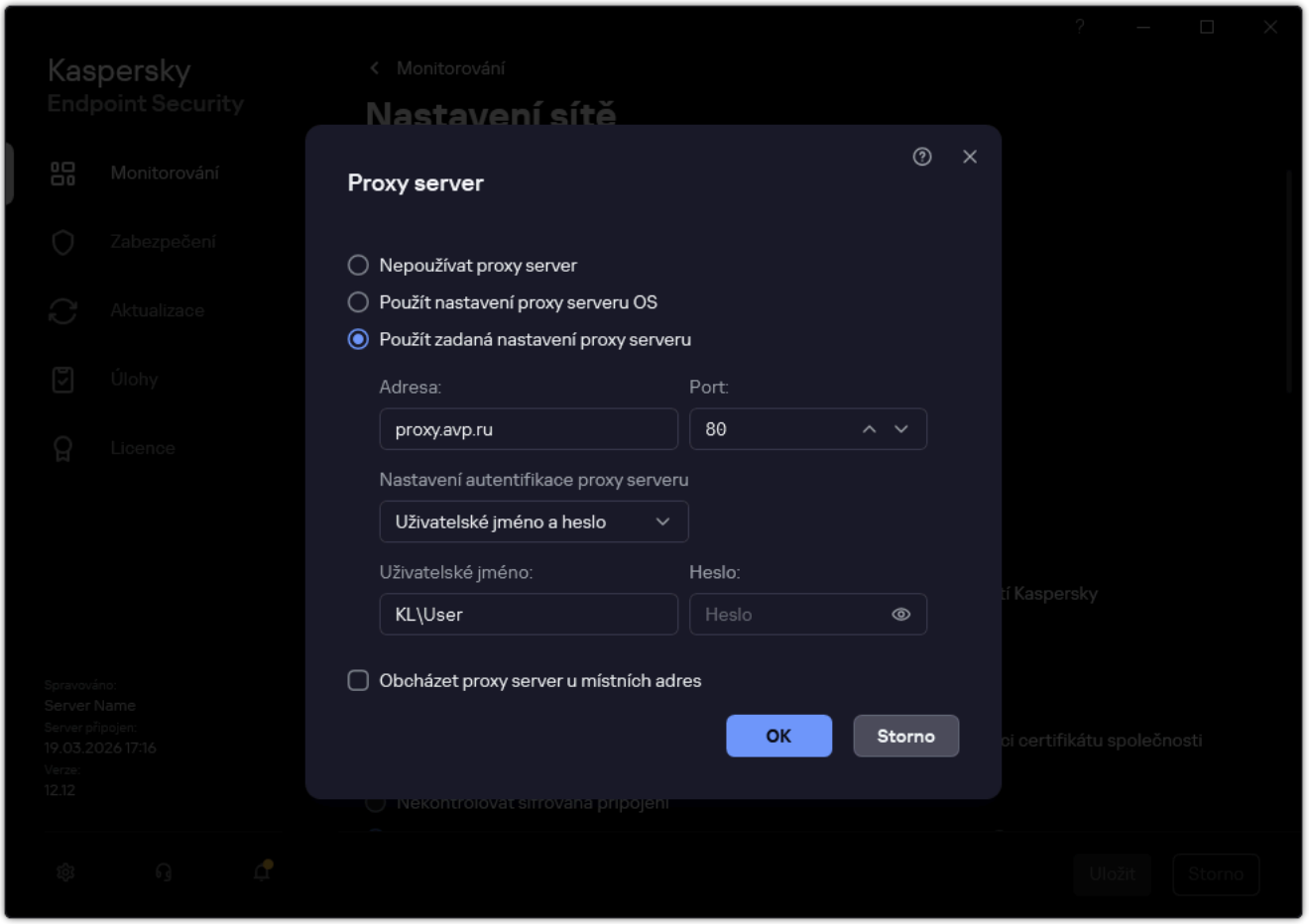
Postup konfigurace nastavení proxy serveru v rozhraní aplikace:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.



Nastavení sítě aplikace

3. V bloku **Proxy server** klikněte na odkaz **Nastavení proxy serveru**.



Nastavení připojení k proxy serveru

4. V okně, které se otevře, vyberte jednu z následujících možností určení adresy proxy serveru:

   - **Použít nastavení proxy serveru OS**.

     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. Vyberte, jak se má aplikace ověřovat na proxy serveru. Ve výchozím nastavení aplikace používá doménové ověřování NTLM aktuálního uživatele.

6. Chcete-li zakázat použití proxy serveru při aktualizaci databází a modulů aplikace ze sdílené složky, zaškrtněte políčko **Obcházet proxy server u místních adres**.

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.

Aplikace Kaspersky Endpoint Security v režimu Light Agent nepodporuje úlohu *Vrácení aktualizace zpět*.

[Jak vrátit nejnovější aktualizaci v konzole pro správu (MMC)]

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

1. Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Vrácení aktualizace zpět**.

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 úloh, například ručně.

Krok 4. Definování názvu úlohy

Zadejte název úlohy.

Krok 7. Dokončení vytvoření úlohy

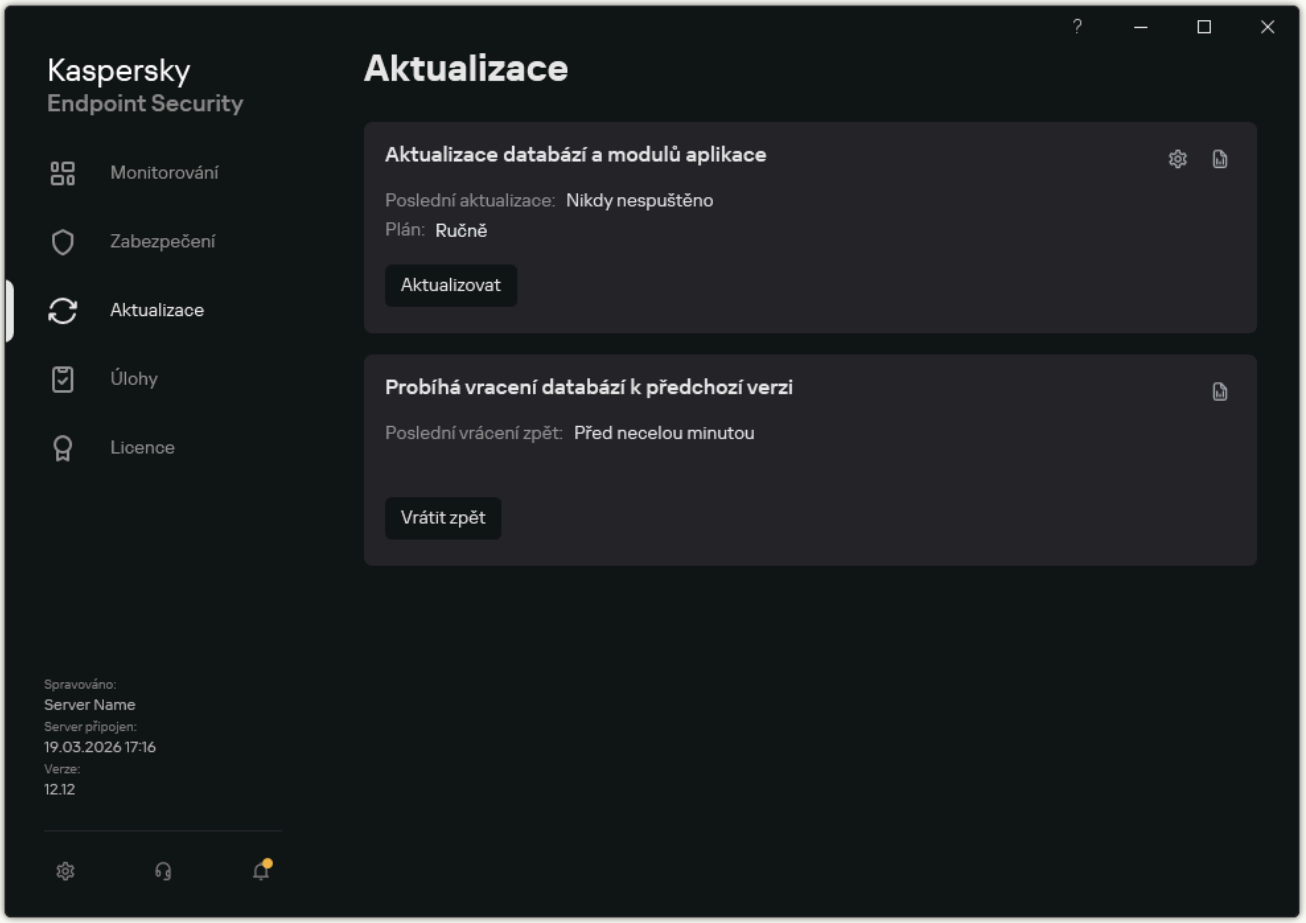
Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak vrátit nejnovější aktualizaci ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Update rollback**.
   c. Do pole **Task name** zadejte krátký popis, například *Vrácení aktualizace*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
7. V seznamu úloh se zobrazí nová úloha.
8. Zaškrtněte políčko vedle úlohy.
9. Klikněte na tlačítko **Start**.

Jak vrátit nejnovější aktualizaci v rozhraní aplikace

1. V hlavním okně aplikace přejděte do části **Aktualizace**.



Úlohy místní aktualizace

2. Na dlaždici **Probíhá vracení 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. Úlohu můžete kdykoli zastavit kliknutím na tlačítko **Zastavit aktualizaci**.

Technologie pokročilé dezinfekce

Pro práci s aktivními hrozbami používá Kaspersky Endpoint Security technologii pokročilé dezinfekce. Pokročilá dezinfekce funguje jinak u pracovních stanic a serverů. Pokročilou dezinfekci můžete nakonfigurovat v nastavení úlohy *Kontrola malwaru* a v nastavení aplikace.

Pokud aplikace Kaspersky Endpoint Security nemůže zastavit provádění malwaru, můžete použít technologii Pokročilá dezinfekce. U počítačů, na které se vztahují zásady, je pokročilá dezinfekce standardně zakázána, protože používá značné množství výpočetních prostředků. U počítačů, na které se nevztahují zásady, je pokročilá dezinfekce ve výchozím nastavení povolena.

Pokročilá dezinfekce funguje jinak u pracovních stanic a serverů. Chcete-li používat tuto technologii na serverech, musíte ve vlastnostech úlohy *Kontrola malwaru* povolit okamžitou pokročilou dezinfekci. Tato podmínka není nutná pro používání této technologie na pracovních stanicích.

Jak povolit nebo zakázat technologii pokročilé dezinfekce v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V bloku **Obecné** pomocí zaškrtávacího políčka **Povolit technologii pokročilé dezinfekce** povolte nebo zakažte technologii pokročilé dezinfekce.

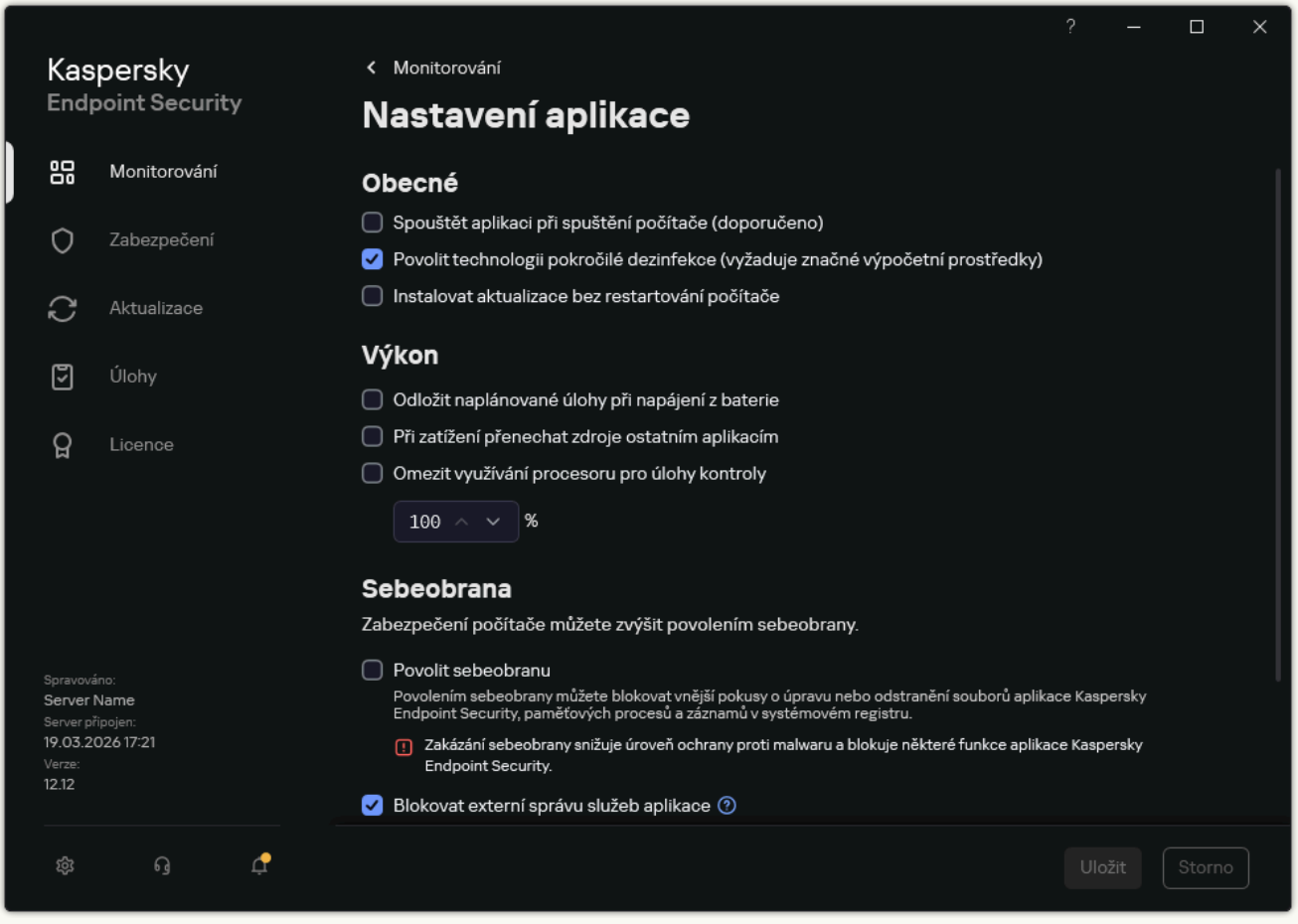
5. Uložte změny.

Jak povolit nebo zakázat technologii pokročilé dezinfekce ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Vyberte **General Settings** → **Detection Settings**.
5. V bloku **Advanced Disinfection Technology** přepínačem **Advanced Disinfection Technology ENABLED** zapněte nebo vypněte technologii pokročilé dezinfekce.
6. Uložte změny.

Jak povolit nebo zakázat technologii pokročilé dezinfekce v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

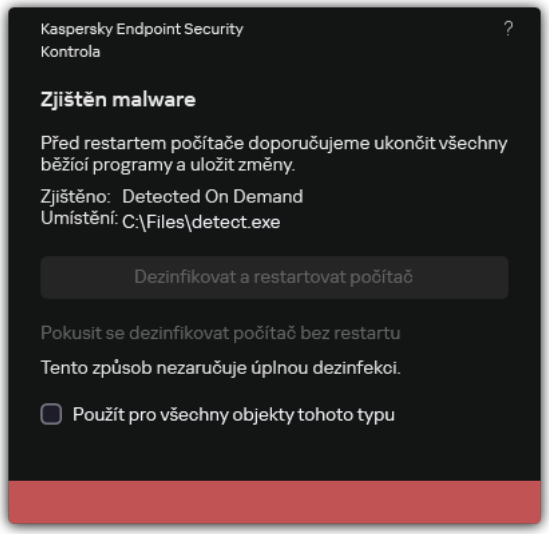
3. V bloku **Obecné** pomocí zaškrtávacího políčka **Povolit technologii pokročilé dezinfekce (vyžaduje značné výpočetní prostředky)** povolte nebo zakažte technologii pokročilé dezinfekce.
4. Uložte změny.

Uživatel tak nemůže využívat většinu funkcí operačního systému, když probíhá pokročilá dezinfekce. Po dokončení dezinfekce se počítač restartuje.

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 *Kontrola malwaru*. Ve vlastnostech úlohy je zaškrtávací políčko **Spustit pokročilou dezinfekci okamžitě**. 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

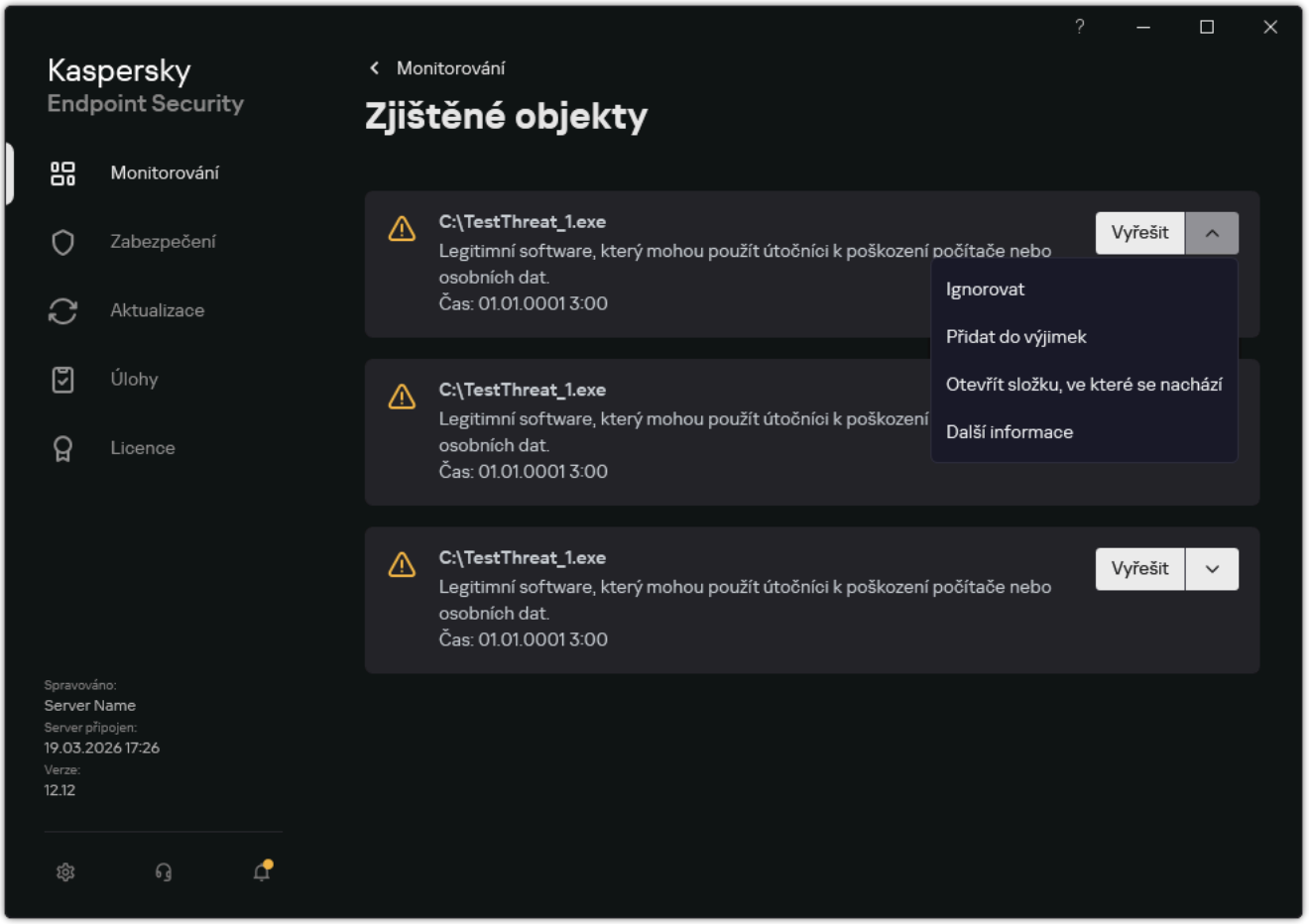
Pro práci s aktivními hrozbami na serverech musíte provést následující:

- povolit technologii Pokročilá dezinfekce v nastavení aplikace;
- povolit okamžitou pokročilou dezinfekci v nastavení úlohy *Kontrola malwaru*.

Je-li aplikace Kaspersky Endpoint Security nainstalována v počítači se systémem Windows pro servery, toto upozornění nezobrazí. Nemůžete tak vybrat akci, která dezinfikuje aktivní hrozbu. Chcete-li dezinfikovat hrozbu, musíte v nastavení aplikace povolit technologii pokročilé dezinfekce a v nastavení úlohy *Kontrola malwaru* povolit okamžitou pokročilou dezinfekci. Poté musíte spustit úlohu *Kontrola malwaru*.

Eliminace nezpracovaných hrozeb

Aplikace Kaspersky Endpoint Security zaznamenává informace o souborech, které nebyly z nějakého důvody zpracovány. Tyto informace se zaznamenávají jako události na seznam aktivních hrozeb (viz obrázek níže).



Seznam aktivních hrozeb

Infikovaný soubor se považuje za *zpracovaný*, pokud jej aplikace Kaspersky Endpoint Security v rámci kontroly počítače na přítomnost virů a jiného malwaru dezinfikovala nebo odstranila hrozbu.

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 nastavení úlohy *Kontrola malwaru* je nastavena akce při zjištění hrozby **Informovat**. Poté, když se na obrazovce zobrazilo oznámení o infikovaném souboru, uživatel vybral možnost **Ignorovat**.

Pokud existují nějaké nezpracované hrozby, aplikace Kaspersky Endpoint Security změní ikonu na . V hlavním okně aplikace se zobrazují upozornění na hrozby (viz obrázek níže). V konzole aplikace Kaspersky Security Center se stav počítače změnil na *Critical* – .

Jak zpracovat hrozbu v konzole pro správu (MMC)

1. V konzole pro správu přejděte do složky **Administration Server** → **Advanced** → **Repositories** → **Active threats**.
   Otevře se seznam aktivních hrozeb.
2. Vyberte objekt, který chcete zpracovat.
3. Vyberte, jak chcete s hrozbou naložit:
   - **Disinfect**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor odstraní.
   - **Delete**. Je-li tato možnost vybrána, aplikace odstraní infikovaný soubor, který je zjištěn z aktivního úložiště hrozeb. V takovém případě aplikace uchová zjištěný soubor v paměti počítače. Chcete-li eliminovat hrozbu z počítače, vyberte možnost **Disinfect**.

Jak zpracovat hrozbu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Operations** → **Repositories** → **Active threats**.

   Otevře se seznam aktivních hrozeb.

2. Vyberte objekt, který chcete zpracovat.

3. Vyberte, jak chcete s hrozbou naložit:

   - **Disinfect**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor odstraní.
   - **Delete**. Je-li tato možnost vybrána, aplikace odstraní infikovaný soubor, který je zjištěn z aktivního úložiště hrozeb. V takovém případě aplikace uchová zjištěný soubor v paměti počítače. Chcete-li eliminovat hrozbu z počítače, vyberte možnost **Disinfect**.

Jak zpracovat hrozbu v rozhraní aplikace

1. V hlavním okně aplikace v části **Monitorování** klikněte na dlaždici **Ochrana je ohrožena**.

   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 se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor odstraní.
   - **Přidat do výjimek**. Pokud je vybrána tato akce, doporučuje Kaspersky Endpoint Security přidání souboru do seznamu výjimek kontroly. Nastavení výjimek se konfiguruje automaticky. Pokud přidání výjimky není dostupné, znamená to, že správce zakázal přidávání výjimek v nastavení zásad.
   - **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 databáze zranitelností a hrozeb společnosti Kaspersky.

Chcete-li zpracovat aktivní hrozby v konzole aplikace Kaspersky Security Center, musíte povolit přenos informací o nezpracovaných souborech na server pro správu. Přenos dat je ve výchozím nastavení povolen.

Jak povolit přenos dat nezpracovaných souborech do konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Zprávy a úložiště**.
4. V bloku **Přenos dat na server pro správu** klikněte na tlačítko **Nastavení**.
5. Zaškrtněte políčko **Nezpracované soubory**.
6. Uložte změny.

Jak povolit přenos dat o nezpracovaných souborech ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

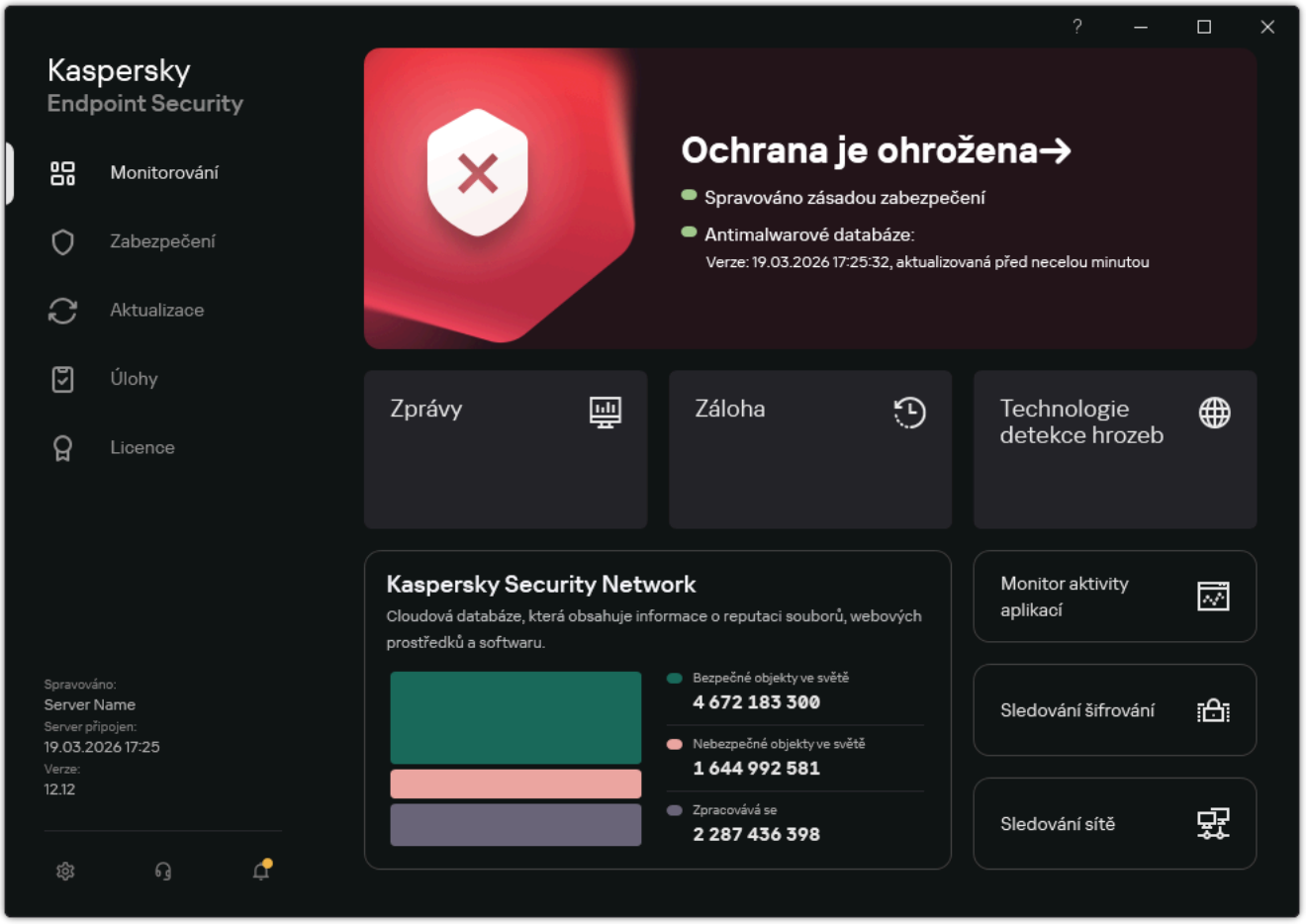
   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **General Settings → KSC Integration**.

5. V bloku **Data transfer to Administration Server** zaškrtněte políčko **About unprocessed files**.

6. Uložte změny.



Hlavní okno aplikace, když je detekována hrozba

Ochrana počítače

Ochrana před souborovými hrozbami

Součást Ochrana před souborovými hrozbami umožňuje zabránit infekci systému souborů počítače. Ve výchozím nastavení je součást Ochrana před souborovými hrozbami trvale umístěna v paměti RAM počítače a v reálném čase kontroluje všechny otevřené, uložené a spuštěné soubory. Součást kontroluje soubory na všech jednotkách počítače včetně připojených jednotek. 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 cloudovém úložišti 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 sady nastavení, které jsou uloženy 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.

Součást Ochrana před souborovými hrozbami používá data přijatá z jiných součástí aplikace. Povolení těchto součástí je volitelné. Mezi součásti, které poskytují další data, patří:

- Kaspersky Security Network.

- Prevence narušení hostitele.
- Detekce chování.

Jak povolit nebo zakázat součást Ochrana před souborovými hrozbami v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
4. Pomocí zaškrtávacího políčka **Ochrana před souborovými hrozbami** můžete tuto součást povolit nebo zakázat.
5. Pokud jste součást povolili, v bloku **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.
     - **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 **Nastavení** a definujte vlastní nastavení součásti.

     Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Výchozí režim**.
6. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory zablokuje (pro čtení/zápis).
   - **Blokovat**. Pokud je vybrána tato možnost, bude součást Ochrana před souborovými hrozbami všechny infikované soubory automaticky blokovat, aniž by se je pokusila dezinfikovat.
   - **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 záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.
7. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před souborovými hrozbami ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **File Threat Protection**.
5. Pomocí přepínače **File Threat Protection ENABLED** můžete tuto součást povolit nebo zakázat.
6. Pokud chcete do rozsahu ochrany přidat nový objekt:

a. V části **Advanced settings** vyberte kartu **Protection scope**.

b. Klikněte na tlačítko **Add**.

c. Tím se otevře okno; v tomto okně vyberte objekty, které chcete přidat do rozsahu ochrany.

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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

Masky můžete použít kdekoli v cestě k souboru nebo složce. Chcete-li například, aby rozsah kontroly zahrnoval složku Stažené soubory pro všechny uživatelské účty v počítači, zadejte masku `C:\Users\*\Downloads\`.

Objekt můžete z ochrany vyloučit, aniž byste jej odebrali ze seznamu objektů v rozsahu ochrany. Chcete-li to provést, přepněte přepínač vedle něj do polohy vypnuto.

d. Uložte změny.

7. V bloku **Action on threat detection** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:

- **Disinfect, delete if disinfection fails**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor odstraní.

- **Disinfect, block if disinfection fails**. 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 zablokuje (pro čtení/zápis).

- **Block**. 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 záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.

8. V případě potřeby upravte pokročilé nastavení ochrany před souborovými hrozbami.

9. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před souborovými hrozbami v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **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 bloku **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.

- **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**.

5. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:

   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory zablokuje (pro čtení/zápis).

   - **Blokovat**. Pokud je vybrána tato možnost, bude součást Ochrana před souborovými hrozbami všechny infikované soubory automaticky blokovat, aniž by se je pokusila dezinfikovat.

   - **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 záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.

6. 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 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 upravené soubory	**Zap**	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.
Používat technologii iSwift	**Zap**	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.
Používat technologii iChecker	**Zap**	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	**Zap**	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
Kontrolovat soubory v poštovním formátu	**Zap**	Kontrolovat soubory v poštovním formátu. Aplikace kontroluje soubory MSG a EML. Soubory v poštovním formátu zahrnují také objekty OLE a soubory MHT. Aplikace Kaspersky Endpoint Security kontroluje soubory ve formátu e-mailu, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
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; a pokud se dezinfekce nezdaří, tak odstranit**	Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Pozastavit součást 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. V bloku **Akce při zjištění hrozby** vyberte příslušnou možnost:
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Je-li tato možnost vybrána, aplikace se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory zablokuje (pro čtení/zápis).
   - **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 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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.

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

4. V bloku **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 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 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. Do pole **Cesta** zadejte cestu ke složce nebo souboru.

   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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

   Masky můžete použít kdekoli v cestě k souboru nebo složce. Chcete-li například, aby rozsah kontroly zahrnoval složku Stažené soubory pro všechny uživatelské účty v počítači, zadejte masku `C:\Users\*\Downloads\`.

   Objekt **Tento počítač** v seznamu souborových prostředků počítače obsahuje následující objekty: **Všechny pevné disky**, **Všechny síťové jednotky** a **Všechny vyměnitelné jednotky**.

   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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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:
   - **Používat technologii 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.
   - **Používat technologii 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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Optimalizace** zaškrtněte políčko **Kontrolovat pouze nové a upravené 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 ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR a ICE a odstraní soubory ve všech jiných formátech (kromě databází pošty).

Postup konfigurace kontroly složených souborů:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Kontrola složených souborů** zadejte typy složených souborů, které chcete kontrolovat: archivy, distribuční balíčky, soubory pošty 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**.

   - **Rozbalovat 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před souborovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **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 provedení**. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich spuštění.

5. Uložte změny.

Kontrola kontejneru

Kontejner je izolované prostředí, ve kterém může být aplikace spuštěna bez přímé interakce s operačním systémem. Používání kontejnerů s sebou nese následující rizika:

- Hackeři mohou být schopni zneužít zranitelnosti kontejnerizace ke kompromitaci aplikací uvnitř kontejneru.
- Hackeři mohou zneužít nezabezpečenou konfiguraci prostředí kontejneru k získání neoprávněného přístupu k datům v počítači nebo k ohrožení integrity systému.
- Úspěšný útok na kontejner může hackerovi umožnit získat přístup k datům v počítači.
- Hackeři mohou zneužít zranitelnosti sítě k zachycení síťového provozu.

Kaspersky Endpoint Security kontroluje soubory nejen na discích, ale také uvnitř kontejnerů. To znamená, že Kaspersky Endpoint Security je externí nástroj pro detekci škodlivé aktivity uvnitř kontejnerů. To umožňuje udržovat výkon kontejnerů a zabraňuje konfliktům s jinými aplikacemi uvnitř kontejneru. Instalace aplikace Kaspersky Endpoint Security do kontejneru není podporována.

Kromě zabezpečení kontejnerů umožňuje Kaspersky Endpoint Security správu aplikací uvnitř kontejnerů součástí Kontrola aplikací. Kontrola aplikací se pro kontejnery konfiguruje stejným způsobem jako pro aplikace nainstalované v počítači. Monitorování integrity systému podporuje také kontejnery.

Požadavky na kontejner

- Kontejner musí být kontejner Docker. Jiné nástroje kontejnerizace nejsou podporovány.
- Kontejner musí běžet v režimu izolace procesu. Režim izolace Hyper-V není podporován.
- Kontejner musí být umístěn na serveru Windows Server 2016, 2019 nebo 2022 (Docker Host).
- Kontejner musí obsahovat bitovou kopii Windows (Docker Image). Windows 10 a 11 nejsou podporovány. Bitové kopie systému Linux nejsou podporovány.

Akce při zjištění hrozby

Pokud je uvnitř kontejneru zjištěna hrozba, aplikace použije akci vybranou pro součást Ochrana před souborovými hrozbami. Kontrola kontejnerů má další nastavení (viz pokyny níže). Pokud je zjištěna hrozba, aplikace zablokuje škodlivou aktivitu a provede vybranou akci (například se pokusí o dezinfekci objektu). Kaspersky Endpoint Security může kontejner zastavit, pokud zjištěný objekt nelze dezinfikovat. Ve výchozím nastavení je funkce zastavování kontejneru zakázána.

Jak konfigurovat kontrolu kontejnerů v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
4. Klikněte na tlačítko **Nastavení**.
5. Tím otevřete okno; v tomto okně vyberte kartu **Rozšířené**.
6. V bloku **Kontrola operací se soubory prováděných v kontejnerech systému Windows** nakonfigurujte nastavení kontroly kontejnerů:
   - **V případě chyby dezinfekce zastavit kontejner**. Aplikace u zjištěného objektu pravděpodobně nemá dostatečná práva pro čtení a zápis. V takovém případě je dezinfekce nebo odstranění zjištěného objektu nemožná. Je-li toto políčko zaškrtnuto, aplikace zablokuje zjištěný objekt a zastaví kontejner. Není-li toto políčko zaškrtnuto, aplikace zablokuje pouze zjištěný objekt.
   - **Nekontrolovat operace se soubory prováděné v kontejnerech systému Windows**. Je-li toto políčko zaškrtnuto, aplikace kontroluje kontejner pouze při jeho spuštění. Pokud toto políčko není zaškrtnuté, aplikace kontroluje kontejner nepřetržitě v reálném čase.
7. Uložte změny.

Jak konfigurovat kontrolu kontejnerů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **File Threat Protection**.
5. V části **Advanced settings** vyberte kartu **Performance**.
6. V bloku **Scan optimization** nakonfigurujte nastavení kontroly kontejnerů:
   - **Stop container if disinfection fails**. Aplikace u zjištěného objektu pravděpodobně nemá dostatečná práva pro čtení a zápis. V takovém případě je dezinfekce nebo odstranění zjištěného objektu nemožná. Je-li toto políčko zaškrtnuto, aplikace zablokuje zjištěný objekt a zastaví kontejner. Není-li toto políčko zaškrtnuto, aplikace zablokuje pouze zjištěný objekt.
   - **Do not scan file operations executed in Windows containers**. Je-li toto políčko zaškrtnuto, aplikace kontroluje kontejner pouze při jeho spuštění. Pokud toto políčko není zaškrtnuté, aplikace kontroluje kontejner nepřetržitě v reálném čase.
7. Uložte změny.

Jak konfigurovat kontrolu kontejnerů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Ochrana před souborovými hrozbami**.
3. V bloku **Kontrola operací se soubory prováděných v kontejnerech systému Windows** nakonfigurujte nastavení kontroly kontejnerů:
   - **V případě chyby dezinfekce zastavit kontejner**. Aplikace u zjištěného objektu pravděpodobně nemá dostatečná práva pro čtení a zápis. V takovém případě je dezinfekce nebo odstranění zjištěného objektu nemožná. Je-li toto políčko zaškrtnuto, aplikace zablokuje zjištěný objekt a zastaví kontejner. Není-li toto políčko zaškrtnuto, aplikace zablokuje pouze zjištěný objekt.
   - **Nekontrolovat operace se soubory prováděné v kontejnerech systému Windows**. Je-li toto políčko zaškrtnuto, aplikace kontroluje kontejner pouze při jeho spuštění. Pokud toto políčko není zaškrtnuté, aplikace kontroluje kontejner nepřetržitě v reálném čase.
4. 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 (například soubory a aplikace)

Síťová aktivita aplikací je ovládána součástí Brána 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 zabezpečení: *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 *Vysoké omezení* je odepřen přístup k modulům operačního systému.

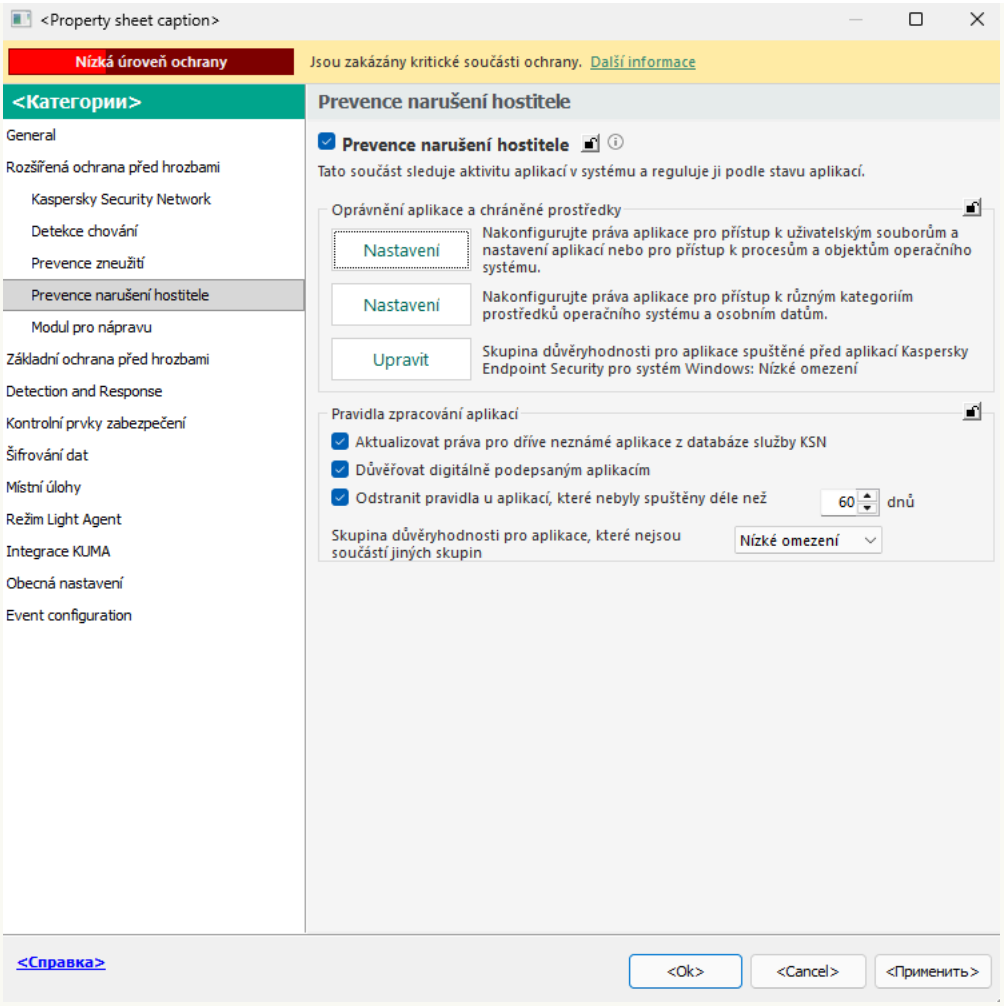
Při příštím spuštění aplikace ověří součást aplikace Kaspersky Endpoint Security integritu aplikace. Pokud je aplikace nezměněná, součást pro ni použije aktuální oprávnění aplikací. Pokud došlo ke změně aplikace, aplikace Kaspersky Endpoint Security analyzuje aplikaci, jako by byla spouštěna poprvé.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. Pomocí zaškrtávacího políčka **Prevence narušení hostitele** můžete tuto součást povolit nebo zakázat.
5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

[Jak povolit nebo zakázat součást Prevence narušení hostitele ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. Pomocí přepínače **Host Intrusion Prevention ENABLED** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

[Jak povolit nebo zakázat součást Prevence narušení hostitele v rozhraní aplikace]

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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 má aplikace Kaspersky Endpoint Security automaticky zařazovat všechny neznámé aplikace. Aplikace, které byly spuštěny před spuštěním aplikace Kaspersky Endpoint Security, jsou automaticky zařazeny do skupiny důvěryhodnosti nastavené v 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 definovanými v nastavení brány firewall.

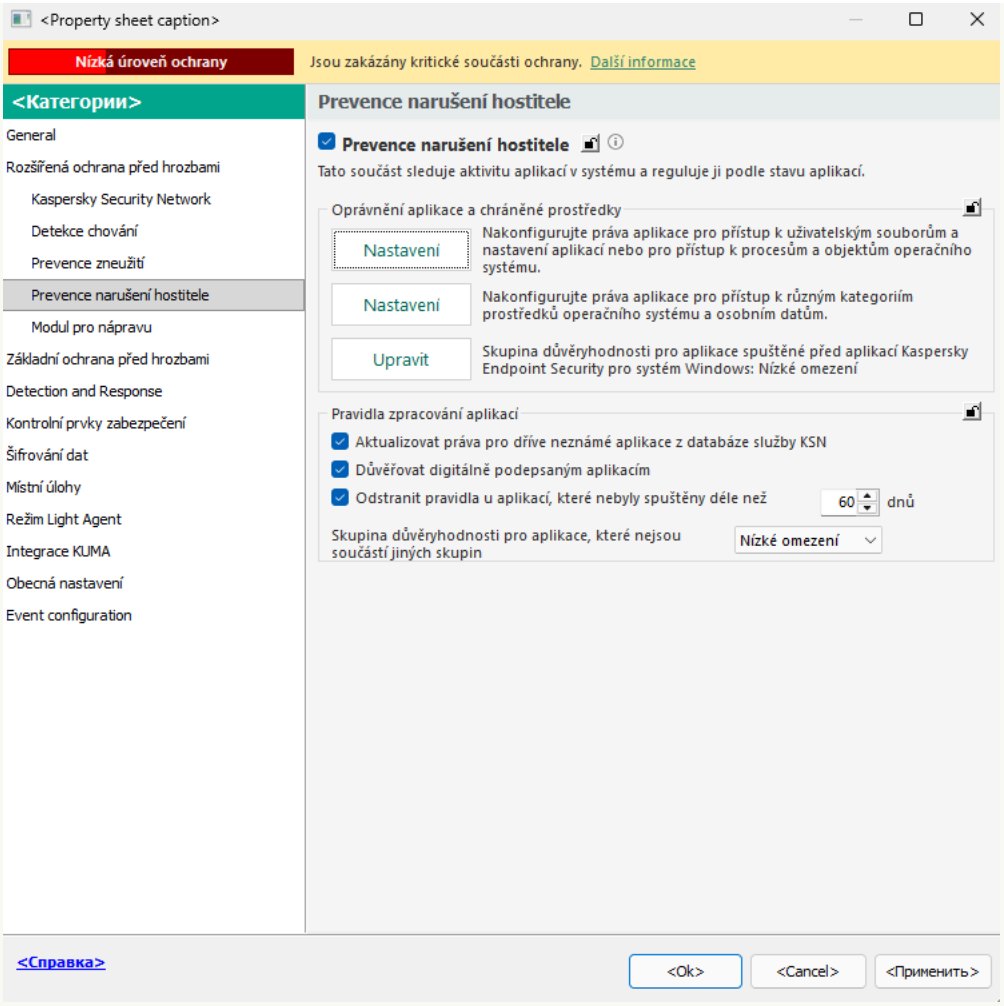
Změna skupiny důvěryhodnosti aplikace

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

5. Vyberte kartu **Oprávnění aplikací**.

6. Klikněte na tlačítko **Přidat**.

7. 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 `?`.

8. Klikněte na tlačítko **Aktualizace**.

   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.

9. Vyberte požadovanou aplikaci.

10. V rozevíracím seznamu **Přidat vybrané aplikace do skupiny důvěryhodnosti** vyberte požadovanou skupinu důvěryhodnosti pro aplikaci.

11. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

[Jak změnit skupinu důvěryhodnosti aplikace ve webové konzole a cloudové konzole](#)

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.

5. V bloku **Application rights and protected resources** klikněte na odkaz **Application rights and protected resources**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

6. Vyberte kartu **Application rights**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.

7. Klikněte na tlačítko **Add**.

   Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.

8. Vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.

9. Vyberte typ **Application**. Přejděte k dalšímu kroku.

   Pokud chcete změnit skupinu důvěryhodnosti pro více aplikací, vyberte typ **Group** 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. Ukončete průvodce.

    Aplikace bude přidána do skupiny důvěryhodnosti.

12. Uložte změny.

Jak změnit skupinu důvěryhodnosti aplikace v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **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 klikněte na **Omezení → <skupina důvěryhodnosti>**.

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 *(definováno 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

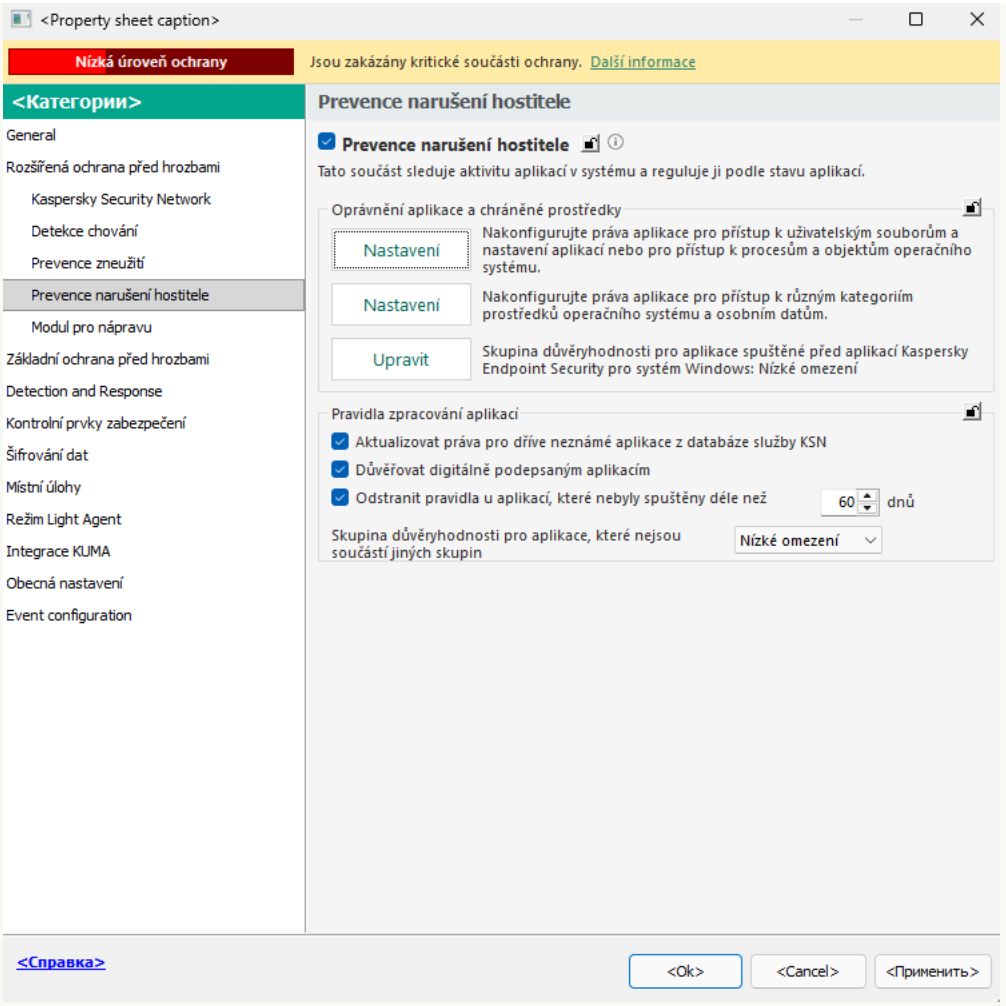
Ve výchozím nastavení jsou vytvořena pro různé skupiny důvěryhodnosti optimální práva aplikace. Nastavení oprávnění skupin aplikací, které jsou ve skupině důvěryhodnosti, dědí hodnoty z nastavení oprávnění skupiny důvěryhodnosti.

Jak změnit práva skupiny důvěryhodnosti v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

5. Přejděte na kartu **Oprávnění aplikací**.

6. Vyberte příslušnou skupinu důvěryhodnosti.

7. V místní nabídce skupiny důvěryhodnosti vyberte možnost **Oprávnění skupin**.

   Tím otevřete vlastnosti skupiny důvěryhodnosti.

8. 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 součástí Brána firewall pomocí *pravidel sítě*.

9. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši, otevřete místní nabídku a vyberte požadovanou možnost: **Dědit**, **Povolit** (✓) nebo **Blokovat** (⊘).

10. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Protokolovat události** (✓/⊘).

    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. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak změnit oprávnění skupiny důvěryhodnosti ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. V bloku **Application rights and protected resources** klikněte na odkaz **Application rights and protected resources**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Přejděte na kartu **Application rights**.

   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 **Files and system registry**.
   - Jestliže chcete upravit oprávnění skupiny důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte možnost **Rights**.

   Síťová aktivita aplikací je ovládána součástí Brána firewall pomocí *pravidel sítě*.
9. U příslušného zdroje ve sloupci odpovídající akce vyberte požadovanou možnost: **Inherit**, **Allow** ( ) nebo **Block** ( ).
10. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Log events** (/).

    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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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:
   - 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 součástí Brána 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 **Zamítnout** ( ).

8. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Protokolovat události** ( ).

   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 (*Vlastní nastavení*).

Výběr skupiny důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security

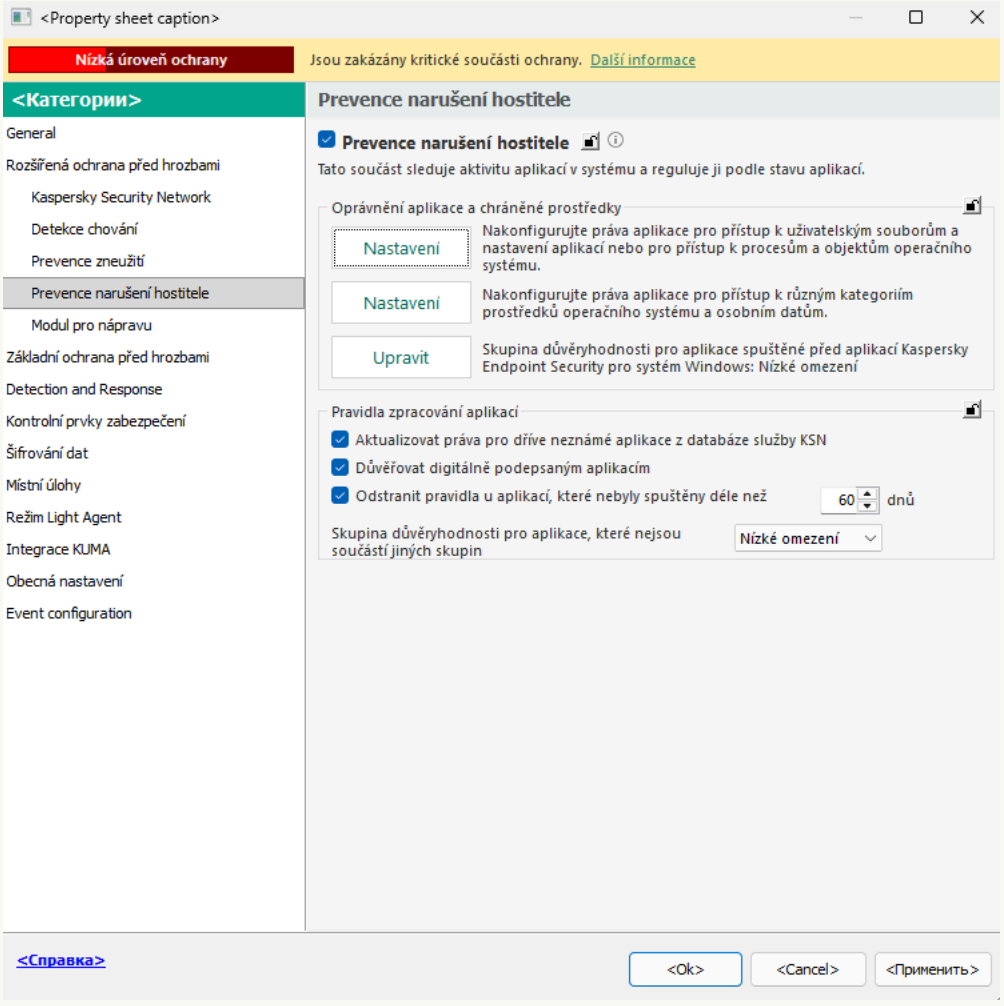
V případě aplikací, které byly spuštěny před aplikací Kaspersky Endpoint Security, je kontrolována pouze síťová aktivita. Kontrola je prováděna v souladu s pravidly sítě definovanými v nastavení brány firewall. Chcete-li určit, která pravidla sítě mají být použita na monitorování síťové aktivity pro tyto aplikace, musíte zvolit skupinu důvěryhodnosti.

Jak vybrat skupinu důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na tlačítko **Upravit**.

5. U nastavení **Trust group for applications started before Kaspersky Endpoint Security** vyberte příslušnou důvěryhodnou skupinu.

6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a 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 **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. U nastavení **Trust group for applications started before Kaspersky Endpoint Security** vyberte příslušnou důvěryhodnou skupinu.
6. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Skupina důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security** vyberte příslušnou důvěryhodnou skupinu.
4. Uložte změny.

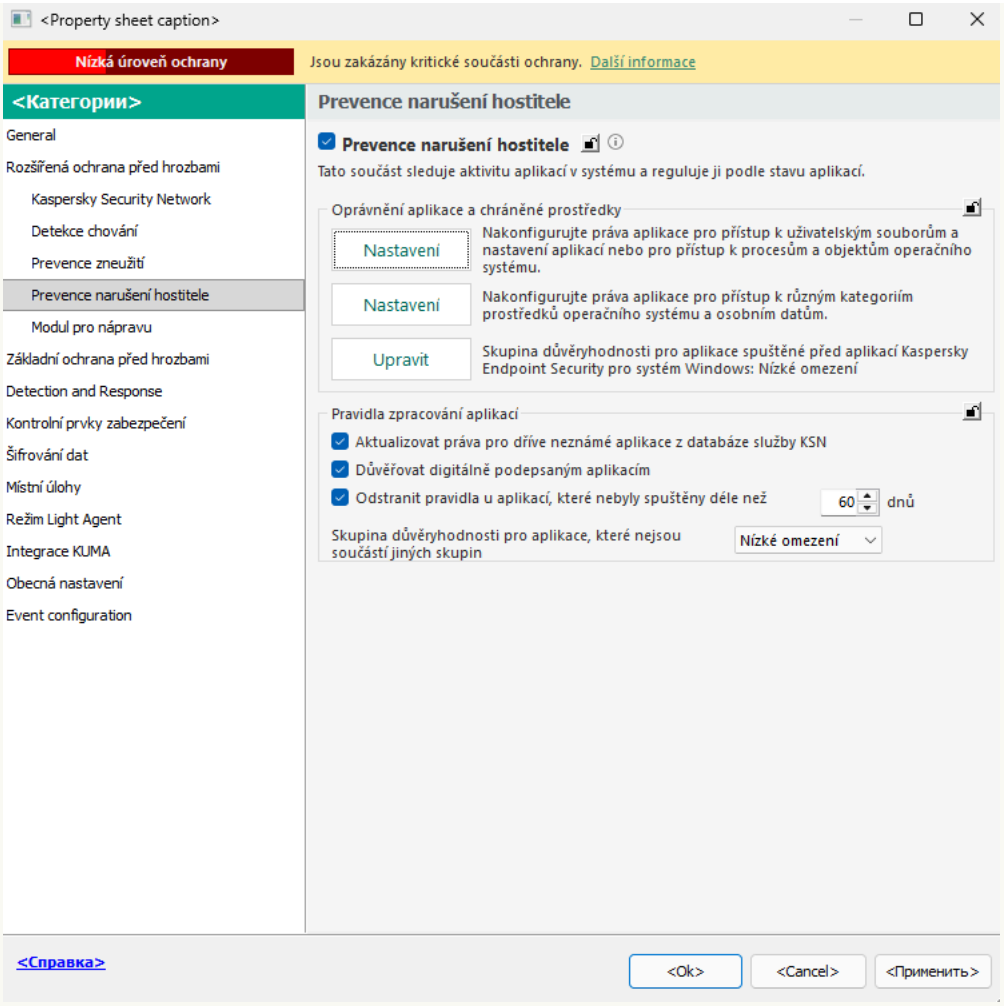
Aplikace spuštěná před aplikací Kaspersky Endpoint Security tak bude zařazena do jiné skupiny důvěryhodnosti. Aplikace Kaspersky Endpoint Security poté zablokuje akce aplikace v závislosti na skupině důvěryhodnosti.

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 *Nízké omezení*. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Application processing rules** pomocí rozevíracího seznamu **Trust group for applications not included in other groups** 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.

5. Pomocí zaškrtávacího políčka **Update rights for previously unknown applications from KSN database** nakonfigurujte automatickou aktualizaci oprávnění neznámých aplikací.

6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak vybrat skupinu důvěryhodnosti pro neznámé aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.

5. V bloku **Application processing rules** pomocí rozevíracího seznamu **Trust group for applications not included in other groups** 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 **Update rights for previously unknown applications from KSN database** nakonfigurujte automatickou aktualizaci oprávnění neznámých aplikací.

7. Uložte změny.

Jak vybrat skupinu důvěryhodnosti pro neznámé aplikace v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.
3. V bloku **Pravidla zpracování aplikací** vyberte příslušnou důvěryhodnou skupinu.

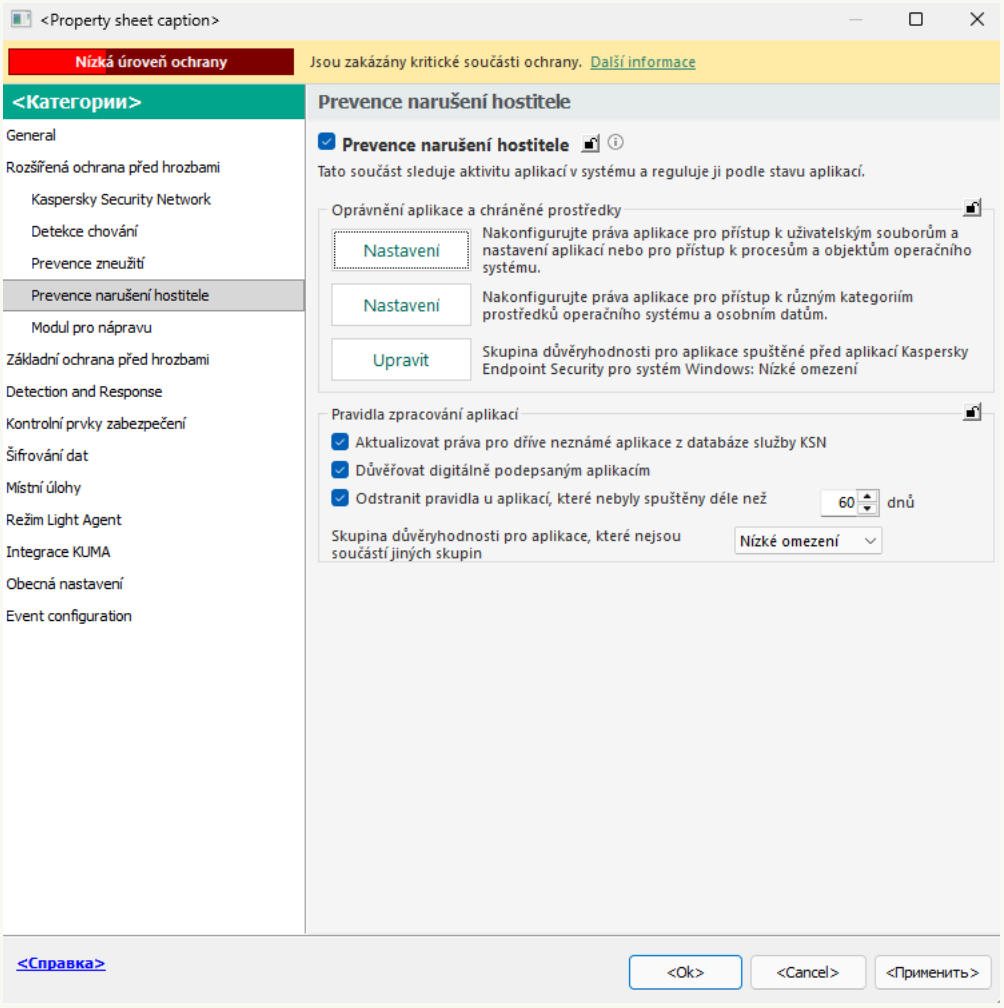
   Pokud je povolena účast ve službě Kaspersky Security Network, aplikace Kaspersky Endpoint Security odešle do služby KSN požadavek ohledně reputace aplikace při každém spuštění aplikace. Na základě obdržené odpovědi může být aplikace přesunuta do jiné skupiny důvěryhodnosti, než jaká je určena v nastavení součásti Prevence narušení hostitele.
4. Pomocí zaškrtávacího políčka **Aktualizovat pravidla pro dříve neznámé aplikace ze 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Application processing rules** pomocí zaškrtávacího políčka **Trust digitally signed applications** povolte nebo zakažte automatické přiřazení skupině důvěryhodnosti Trusted 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.

5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak vybrat skupinu důvěryhodnosti pro digitálně podepsané aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. V bloku **Application processing rules** pomocí zaškrtávacího políčka **Trust digitally signed applications** povolte nebo zakažte automatické přiřazení skupině důvěryhodnosti Trusted 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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Application processing rules** pomocí zaškrtávacího políčka **Trust digitally signed applications** povolte nebo zakažte automatické přiřazení skupině důvěryhodnosti Trusted 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

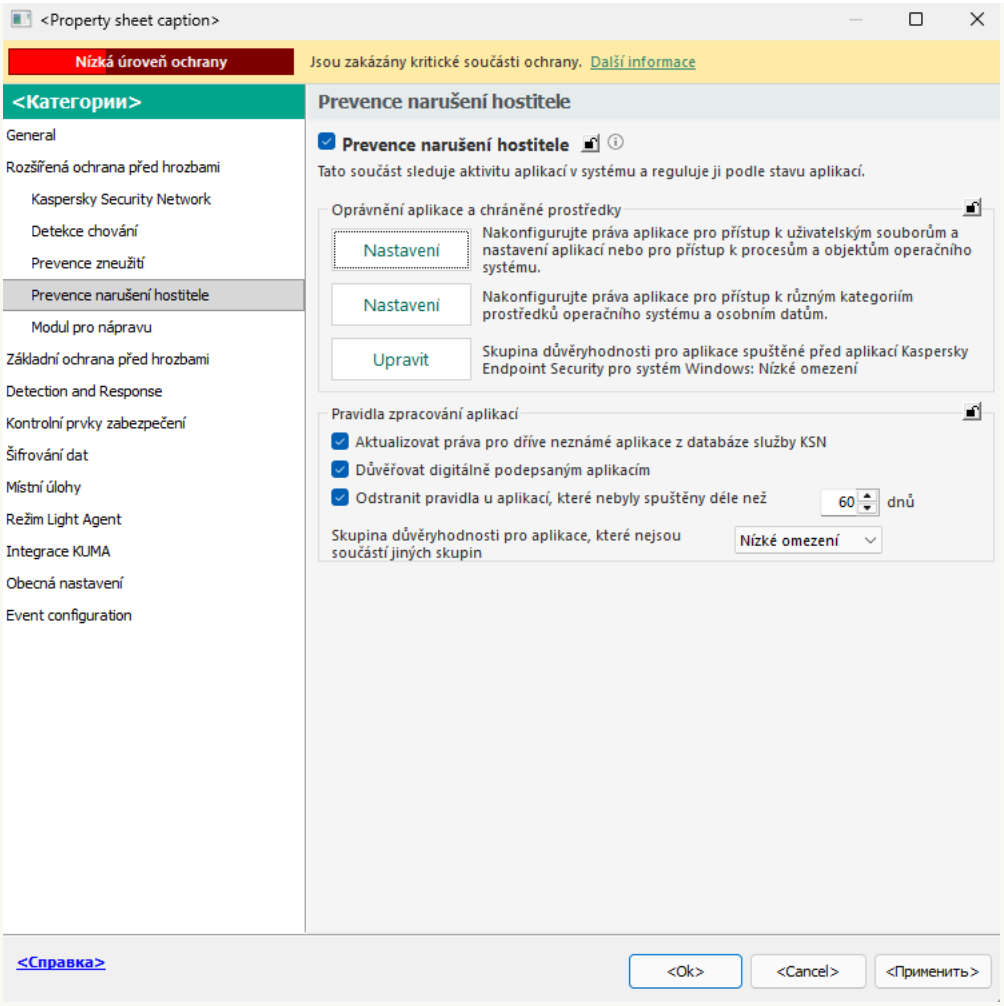
Ve výchozím nastavení je aktivita aplikace řízena na základě práv aplikace definovaných pro konkrétní skupinu důvěryhodnosti, kterou aplikace Kaspersky Endpoint Security přiřadila aplikaci při jejím prvním spuštění. Pokud je to nutné, můžete oprávnění aplikací upravit pro celou skupinu důvěryhodnosti, 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. Když není aplikace podřízenou aplikací aplikace, ze které běží, pravidla se nezdědí.

Jak změnit oprávnění aplikací v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

5. Přejděte na kartu **Oprávnění aplikací**.

6. Klikněte na tlačítko **Přidat**.

7. V okně, které se otevře, zadejte kritéria pro vyhledání aplikace, jejíž oprávnění aplikace chcete změnit.

   Můžete zadat název aplikace nebo název dodavatele. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

8. Klikněte na tlačítko **Aktualizace**.

   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.

9. Vyberte požadovanou aplikaci.

10. V rozevíracím seznamu **Přidat vybrané aplikace do skupiny důvěryhodnosti** vyberte položku **Výchozí skupiny** a klikněte na tlačítko **OK**.

    Aplikace bude přidána do výchozí skupiny.

11. Vyberte příslušnou aplikaci a poté vyberte možnost **Oprávnění aplikací** v místní nabídce aplikace.

    Otevřou se vlastnosti aplikace.

12. 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 součástí Brána firewall pomocí *pravidel sítě*.

13. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši, otevřete místní nabídku a vyberte požadovanou možnost: **Dědit**, **Povolit** (✓) nebo **Blokovat** (⊘).
14. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Protokolovat události** (✓/⊘).

    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.
15. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak změnit oprávnění aplikací ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

    Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. V bloku **Application rights and protected resources** klikněte na odkaz **Application rights and protected resources**.

    Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Přejděte na kartu **Application rights**.

    Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.
7. Klikněte na tlačítko **Add**.

    Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.
8. Vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.
9. Vyberte typ **Application**. Přejděte k dalšímu kroku.

    Pokud chcete změnit skupinu důvěryhodnosti pro více aplikací, vyberte typ **Group** 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. Ukončete průvodce.

    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 **Files and system registry**.
    - Jestliže chcete upravit oprávnění skupiny důvěryhodnosti, která regulují přístup k procesům a objektům operačního systému, vyberte možnost **Rights**.

    Síťová aktivita aplikací je ovládána součástí Brána firewall pomocí *pravidel sítě*.
14. U příslušného zdroje ve sloupci odpovídající akce vyberte požadovanou možnost: **Inherit**, **Allow** (✓) nebo **Block** (✗).
15. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Log events** (✓/✗).

    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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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:
   - 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**.
7. U příslušného zdroje ve sloupci odpovídající akce klikněte pravým tlačítkem myši, otevřete místní nabídku a vyberte požadovanou možnost: **Dědit**, **Povolit** (✓) nebo **Zamítnout** (!).
8. Chcete-li sledovat využití počítačových zdrojů, vyberte možnost **Protokolovat události** (📊).

   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

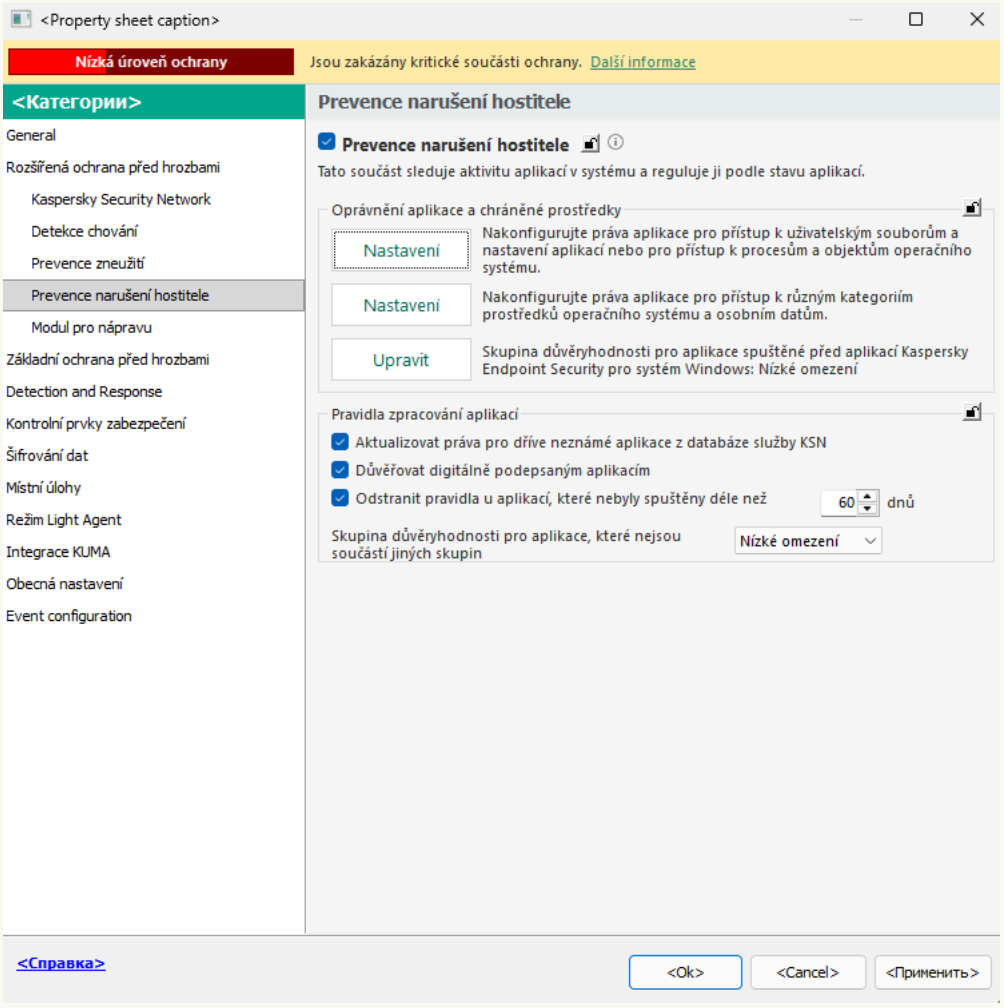
Parametr	Popis
Nekontrolovat soubory, které otevírá tato aplikace	Z kontroly aplikací Kaspersky Endpoint Security jsou vyloučeny všechny soubory, které otevírá tato aplikace. Pokud například používáte aplikace k zálohování souborů, tato funkce pomáhá snížit spotřebu prostředků aplikací Kaspersky Endpoint Security.
Nemonitorovat činnost aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat souborovou ani síťovou aktivitu aplikace v operačním systému. Monitorování aktivity aplikací můžete nakonfigurovat pro různé součásti aplikace Kaspersky Endpoint Security: • **Nemonitorovat u součástí ochrany a kontroly**. Činnost aplikace je monitorována následujícími součástmi: Detekce chování, Prevence zneužití, Prevence narušení hostitele, Modul pro nápravu a Brána firewall. • **Nemonitorovat u řešení Managed Detection and Response a Endpoint Detection and Response**. Aktivitu aplikace monitoruje integrovaný agent MDR a integrovaný agent EDR (KATA). • **Nezachytávat interaktivní vstup konzoly u řešení Endpoint Detection and Response**. Kaspersky Endpoint Security neodesílá telemetrická data o správě aplikace na konzole. Telemetrická data používá platformou Kaspersky Anti Targeted Attack Platform (EDR).
Nedědit omezení z 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).
Nemonitorovat činnost podřízené aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu souborů ani síťovou aktivitu aplikací spuštěných touto aplikací. Výjimku můžete použít rekurzivně. Aplikace tak nebude monitorovat činnost celého řetězce podřízených 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. Pokud je pro důvěryhodnou aplikaci místo cesty zadána hodnota hash, aplikace nepodporuje vyloučení síťového provozu.

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 Po 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Oprávnění aplikace a chráněné prostředky** klikněte na tlačítko **Nastavení**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

5. Přejděte na 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.

6. Vyberte kategorii chráněných prostředků, do nichž chcete přidat nový chráněný prostředek.

   Chcete-li přidat podkategorii, klikněte na položky **Přidat → Kategorie**.

7. Klikněte na tlačítko **Přidat**. V rozevíracím seznamu vyberte typ prostředku, který chcete přidat: **Soubor nebo složka** nebo **Klíč registru**.

8. 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.

9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak přidat chráněný prostředek ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. V bloku **Application rights and protected resources** klikněte na odkaz **Application rights and protected resources**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.
6. Přejděte na kartu **Protected resources**.

   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 **Add**.

   Spustí se průvodce novým prostředkem.
8. V bloku **Group name** vyberte kategorii chráněných prostředků, do nichž chcete přidat nový chráněný prostředek.

   Pokud chcete přidat podkategorii, vyberte možnost **Category of protected resources**.
9. Vyberte typ prostředku, který chcete přidat: **File or folder** nebo **Registry key**.
10. Vyberte soubor, složku nebo klíč registru.
11. Ukončete průvodce.

    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 **Status** a deaktivovat řízení aktivity aplikace s prostředky.
12. Uložte změny.

Jak přidat chráněný prostředek v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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 **Povolit 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.

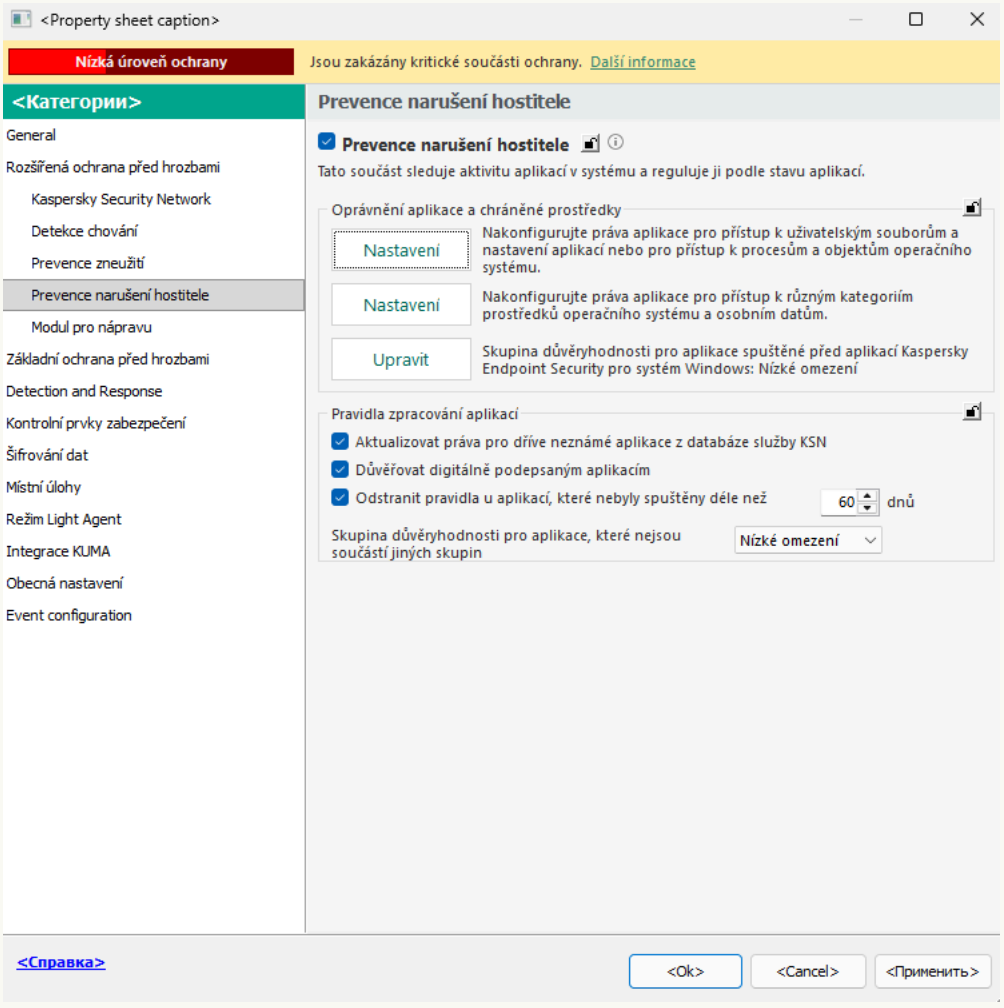
Aplikace Kaspersky Endpoint Security automaticky odstraňuje informace o nepoužitých aplikacích a šetří tak prostředky počítače. Aplikace Kaspersky Endpoint Security odstraňuje informace o aplikaci podle následujících pravidel:

- 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence narušení hostitele**.



Nastavení součásti Prevence narušení

4. V bloku **Pravidla zpracování aplikací** proveďte některou z následujících akcí:
   - Pokud chcete konfigurovat automatické odstraňování, zaškrtněte políčko **Odstranit pravidla u aplikací, které nebyly spuštěny déle než N dnů** a zadejte 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, zrušte zaškrtnutí políčka **Odstranit pravidla u aplikací, které nebyly spuštěny déle než N dnů**.

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.

5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

[Jak nakonfigurovat automatické odstraňování informací o nepoužívaných aplikacích ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Host Intrusion Prevention**.
5. V bloku **Application processing rules** proveďte některou z následujících akcí:
   - Pokud chcete konfigurovat automatické odstraňování, zaškrtněte políčko **Delete rules for applications that have not been started for longer than (days, 1 to 90)** a zadejte 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, zrušte zaškrtnutí políčka **Delete rules for applications that have not been started for longer than (days, 1 to 90)**.

     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 hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Prevence narušení hostitele**.
3. V bloku **Pravidla zpracování aplikací** proveďte některou z následujících akcí:
   - Pokud chcete konfigurovat automatické odstraňování, zaškrtněte políčko **Odstranit pravidla u aplikací, které nebyly spuštěny déle než N dny (od 1 do 90)** a zadejte 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, zrušte zaškrtnutí políčka **Odstranit pravidla u aplikací, které nebyly spuštěny déle než N dny (od 1 do 90)**.

     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

Funkce ochrany zvukového signálu a funkce ochrany přístupu k webové kameře nejsou podporovány na počítačích s architekturou ARM.

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 aplikace Kaspersky Endpoint Security umožňuje příjem audio a video streamů pouze pro aplikace ze skupiny *Důvěryhodné*. Aplikace ze skupin *Nízké omezení*, *Vysoké omezení* a *Nedůvěryhodné* nemají povoleno přijímat audio a video stream 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.

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 klávesnice 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 opětovné autorizaci této klávesnice.

Pokud číselný kód zadáte nesprávně, aplikace vygeneruje nový kód. Můžete nakonfigurovat počet pokusů o zadání numerického kódu. Pokud byl numerický kód zadán vícekrát nesprávně nebo bylo zavřeno okno autorizace klávesnice (viz obrázek níže), aplikace zablokuje vstup z této klávesnice. Když vyprší doba blokování zařízení USB 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.

Jak povolit nebo zakázat součást Ochrana před útoky BadUSB v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před útoky BadUSB**.
4. Pomocí zaškrtávacího políčka **Ochrana před útoky BadUSB** můžete tuto součást povolit nebo zakázat.

5. V bloku **Povolení zařízení USB po připojení** upravte nastavení zabezpečení pro zadání ověřovacího kódu:

   - **Maximální počet pokusů o ověření zařízení USB**. Automatické blokování zařízení USB, pokud je zadaný ověřovací kód nesprávně zadán několikrát. Platné hodnoty jsou 1 až 10. Pokud například povolíte pět pokusů o zadání ověřovacího kódu, aplikace zařízení USB po pátém neúspěšném pokusu zablokuje. Aplikace Kaspersky Endpoint Security zobrazí dobu blokování zařízení USB. Po uplynutí této doby máte pět pokusů o zadání ověřovacího kódu.

   - **Časový limit při dosažení maximálního počtu pokusů (minuty)**. Doba blokování zařízení USB po zadaném počtu neúspěšných pokusů o zadání ověřovacího kódu. Platné hodnoty jsou 1 až 180 (minuty).

6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Ochrana před útoky BadUSB ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection** → **BadUSB Attack Prevention**.

5. Pomocí přepínače **BadUSB Attack Prevention ENABLED** můžete tuto součást povolit nebo zakázat.

6. V bloku **Authorization of USB devices** upravte nastavení zabezpečení pro zadání ověřovacího kódu:

   - **Maximum number of USB device authorization attempts**. Automatické blokování zařízení USB, pokud je zadaný ověřovací kód nesprávně zadán několikrát. Platné hodnoty jsou 1 až 10. Pokud například povolíte pět pokusů o zadání ověřovacího kódu, aplikace zařízení USB po pátém neúspěšném pokusu zablokuje. Aplikace Kaspersky Endpoint Security zobrazí dobu blokování zařízení USB. Po uplynutí této doby máte pět pokusů o zadání ověřovacího kódu.

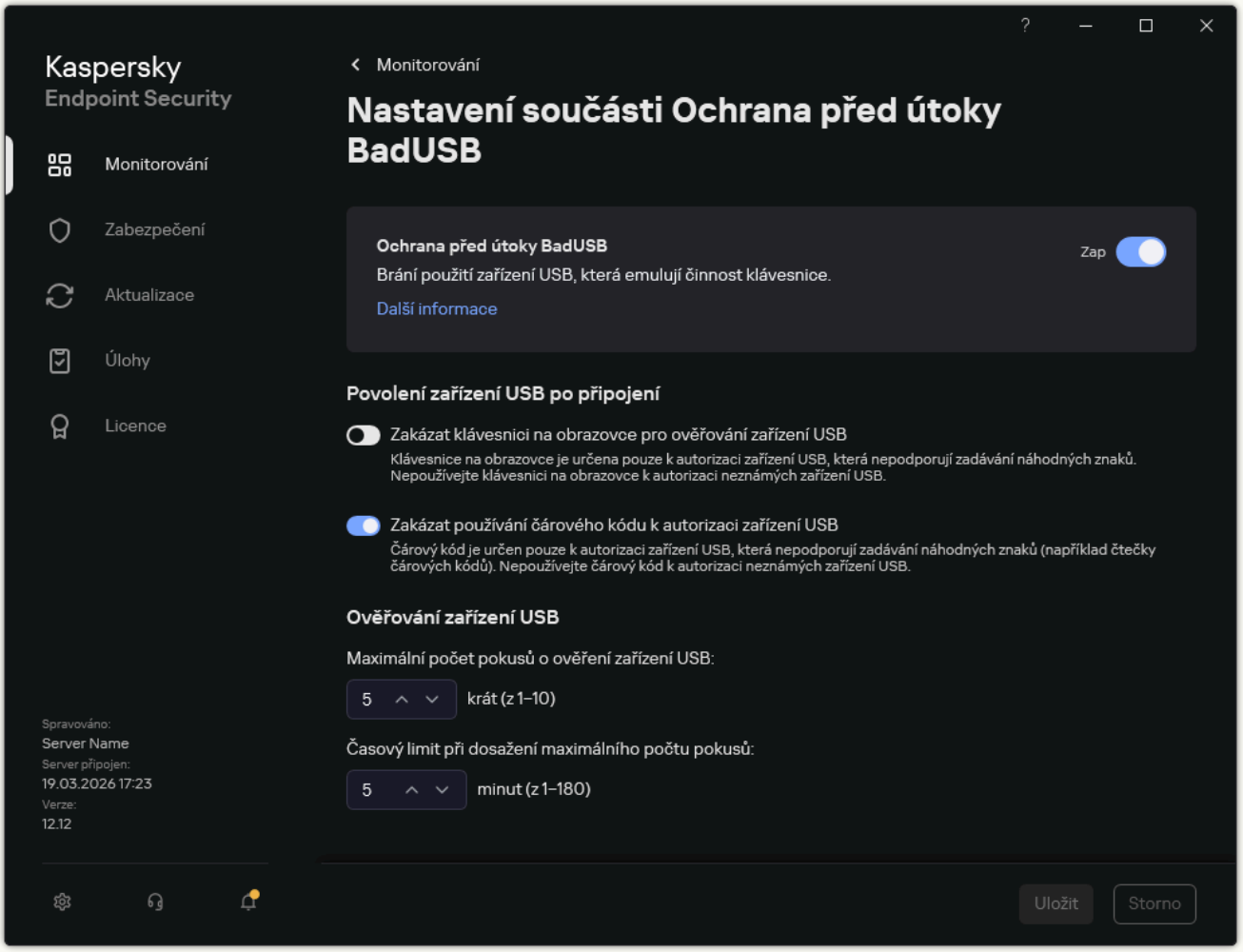
   - **Timeout when reaching the maximum number of attempts (min)**. Doba blokování zařízení USB po zadaném počtu neúspěšných pokusů o zadání ověřovacího kódu. Platné hodnoty jsou 1 až 180 (minuty).

7. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před útoky BadUSB v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Ochrana před útoky BadUSB**.



Nastavení součásti Ochrana před útoky BadUSB

3. Pomocí přepínače **Ochrana před útoky BadUSB** můžete tuto součást povolit nebo zakázat.

4. V bloku **Povolení zařízení USB po připojení** upravte nastavení zabezpečení pro zadání ověřovacího kódu:

   - **Maximální počet pokusů o ověření zařízení USB**. Automatické blokování zařízení USB, pokud je zadaný ověřovací kód nesprávně zadán několikrát. Platné hodnoty jsou 1 až 10. Pokud například povolíte pět pokusů o zadání ověřovacího kódu, aplikace zařízení USB po pátém neúspěšném pokusu zablokuje. Aplikace Kaspersky Endpoint Security zobrazí dobu blokování zařízení USB. Po uplynutí této doby máte pět pokusů o zadání ověřovacího kódu.

   - **Časový limit při dosažení maximálního počtu pokusů**. Doba blokování zařízení USB po zadaném počtu neúspěšných pokusů o zadání ověřovacího kódu. Platné hodnoty jsou 1 až 180 (minuty).

5. 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.

Jak povolit nebo zakázat použití klávesnice na obrazovce pro autorizaci v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před útoky BadUSB**.

4. Prostřednictvím políčka **Zakázat použití klávesnice na obrazovce k autorizaci zařízení USB** můžete blokovat nebo povolit používání klávesnice na obrazovce k autorizaci.

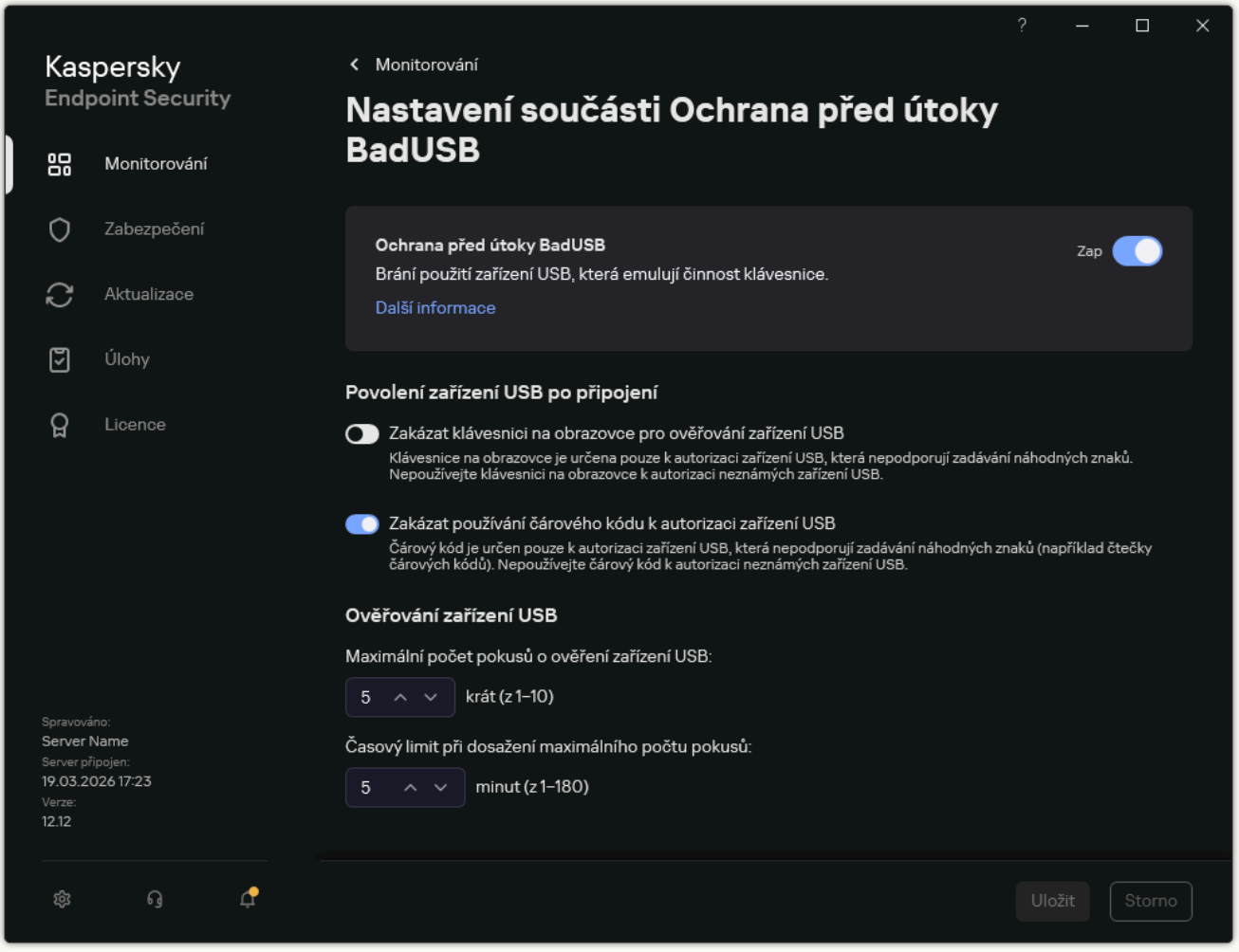
5. Uložte změny.

Jak povolit nebo zakázat použití klávesnice na obrazovce pro autorizaci ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Prostřednictvím přepínače **Prohibit use of On-Screen Keyboard for authorization of USB devices** můžete blokovat nebo povolit používání klávesnice na obrazovce k autorizaci.
6. Uložte změny.

Jak povolit nebo zakázat použití klávesnice na obrazovce pro autorizaci v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Ochrana před útoky BadUSB**.



Nastavení součásti Ochrana před útoky BadUSB

3. Prostřednictvím přepínače **Zakázat klávesnici na obrazovce pro ověřování zařízení USB** můžete blokovat nebo povolit používání klávesnice na obrazovce k autorizaci.
4. Uložte změny.



Ověřování zařízení USB

Autorizace čtečky čárových kódů

Při připojování čtečky čárových kódů k počítači součást Ochrana před útoky BadUSB identifikuje toto zařízení jako vstupní zařízení a vyzve vás k provedení autorizace. Chcete-li čtečku čárových kódů autorizovat, musíte naskenovat čárový kód zobrazený na obrazovce. Aplikace vygeneruje čárový kód ve formátu Code39, který podporuje většina čteček čárových kódů a QR kódů.

Kaspersky Endpoint Security také podporuje jinou metodu autorizace skeneru čárových kódů. Pokud používáte zařízení s dotykovou obrazovkou, můžete k zadání kódu použít klávesnici na obrazovce. Chcete-li tak učinit, musíte povolit klávesnici na obrazovce. Tento způsob je vhodný například v případě stacionárních snímačů čárových kódů zabudovaných v pokladnách. Jiné způsoby autorizace čtečky čárových kódů jsou zakázány.

Ve výchozím nastavení aplikace nepoužívá pro autorizaci zařízení USB čárový kód.

Jak povolit nebo zakázat autorizaci čárovým kódem v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před útoky BadUSB**.
5. Prostřednictvím políčka **Zakázat používání čárového kódu k autorizaci zařízení USB** můžete blokovat nebo povolit používání čárového kódu k autorizaci.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

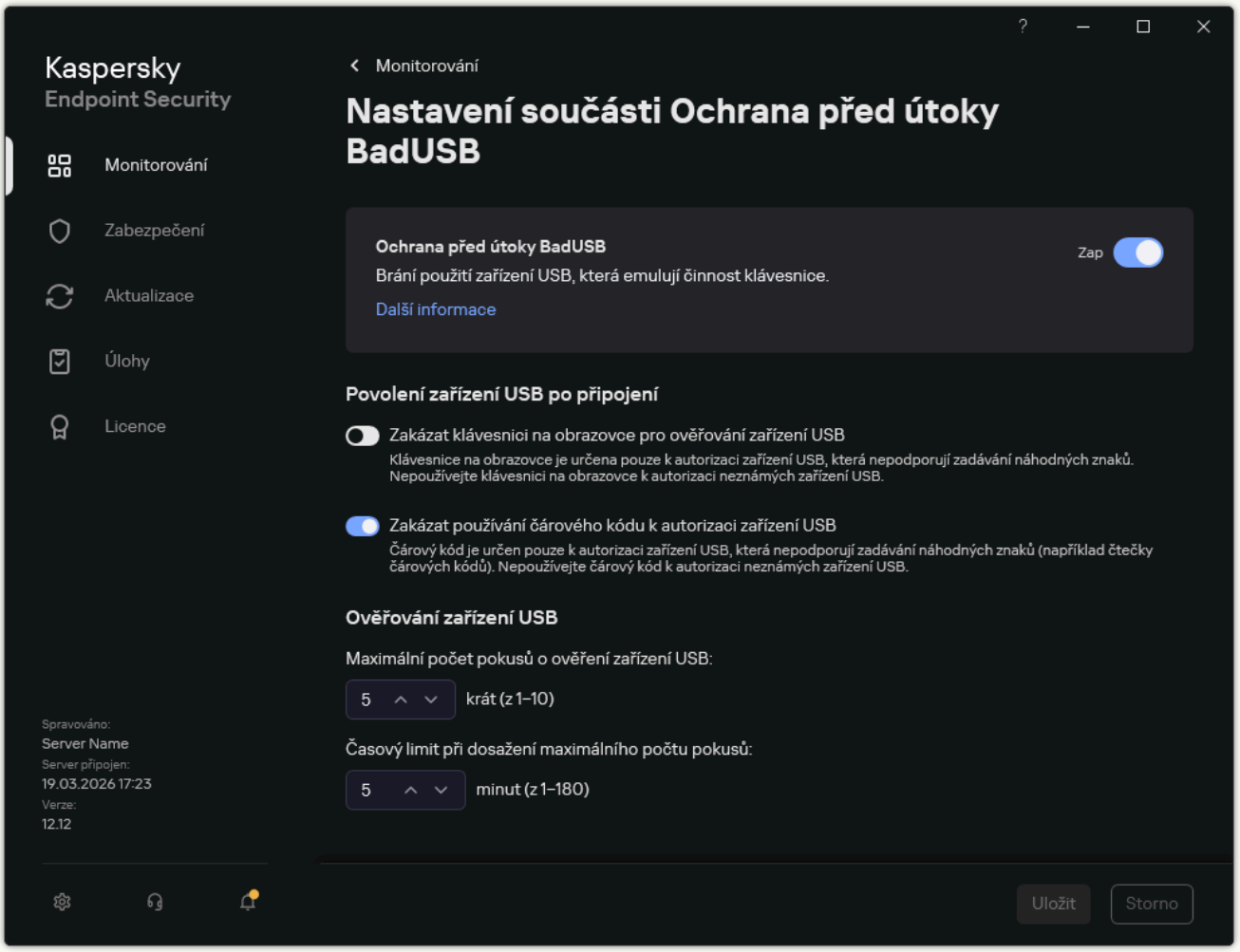
Jak povolit nebo zakázat autorizaci čárovým kódem ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection → BadUSB Attack Prevention**.
5. Prostřednictvím přepínače **Prohibit use of a barcode for authorization of USB devices** můžete blokovat nebo povolit používání čárového kódu k autorizaci.

6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

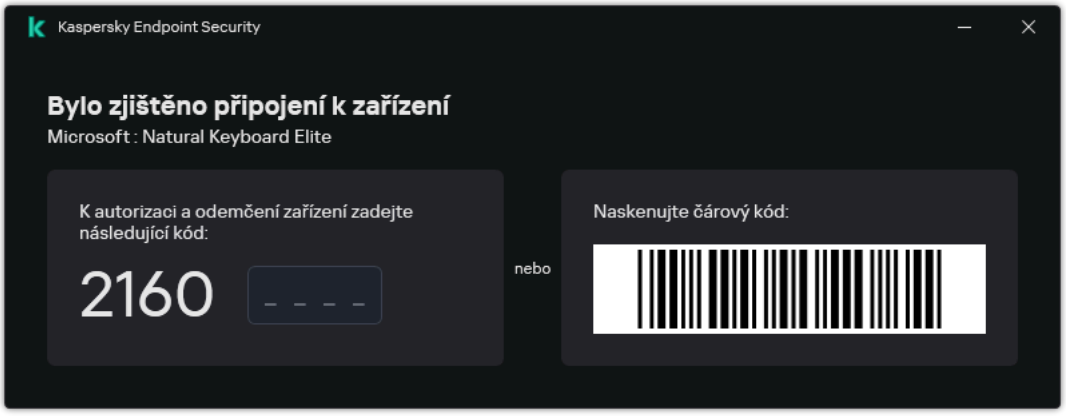
Jak povolit autorizaci zařízení USB pomocí čárového kódu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před útoky BadUSB**.



Nastavení součásti Ochrana před útoky BadUSB

3. Prostřednictvím přepínače **Zakázat používání čárového kódu k autorizaci zařízení USB** můžete blokovat nebo povolit používání čárového kódu k autorizaci.
4. Uložte změny.

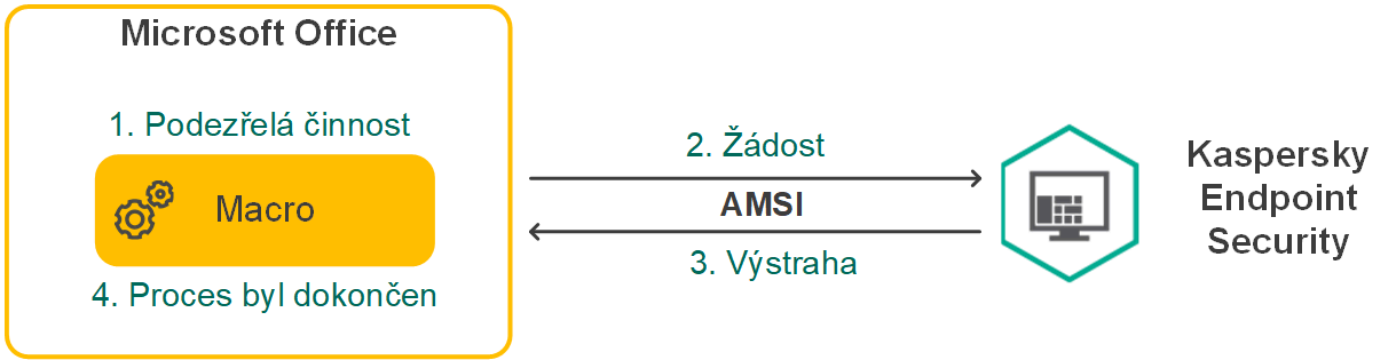


Autorizace čtečky čárových kódů

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 upozornění na hrozbu nepovolí provedení škodlivých akcí (například akci 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 neodmítá požadavky od aplikací třetích stran, pro které je povolena nepřetržitá integrace 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 / více relací Enterprise;
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (včetně režimu Server Core);
- Windows Server 2025 Standard / Datacenter.

Povolení a zakázání součásti Ochrana AMSI

Ve výchozím nastavení je součást Ochrana AMSI povolena a funguje v režimu doporučeném společností Kaspersky (viz tabulka níže).

Jak povolit nebo zakázat součást Ochrana AMSI v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Nástroj pro kontrolu AMSI**.
4. Pomocí zaškrtávacího políčka **Nástroj pro kontrolu AMSI** můžete tuto součást povolit nebo zakázat.
5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Ochrana AMSI ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection → AMSI Protection**.

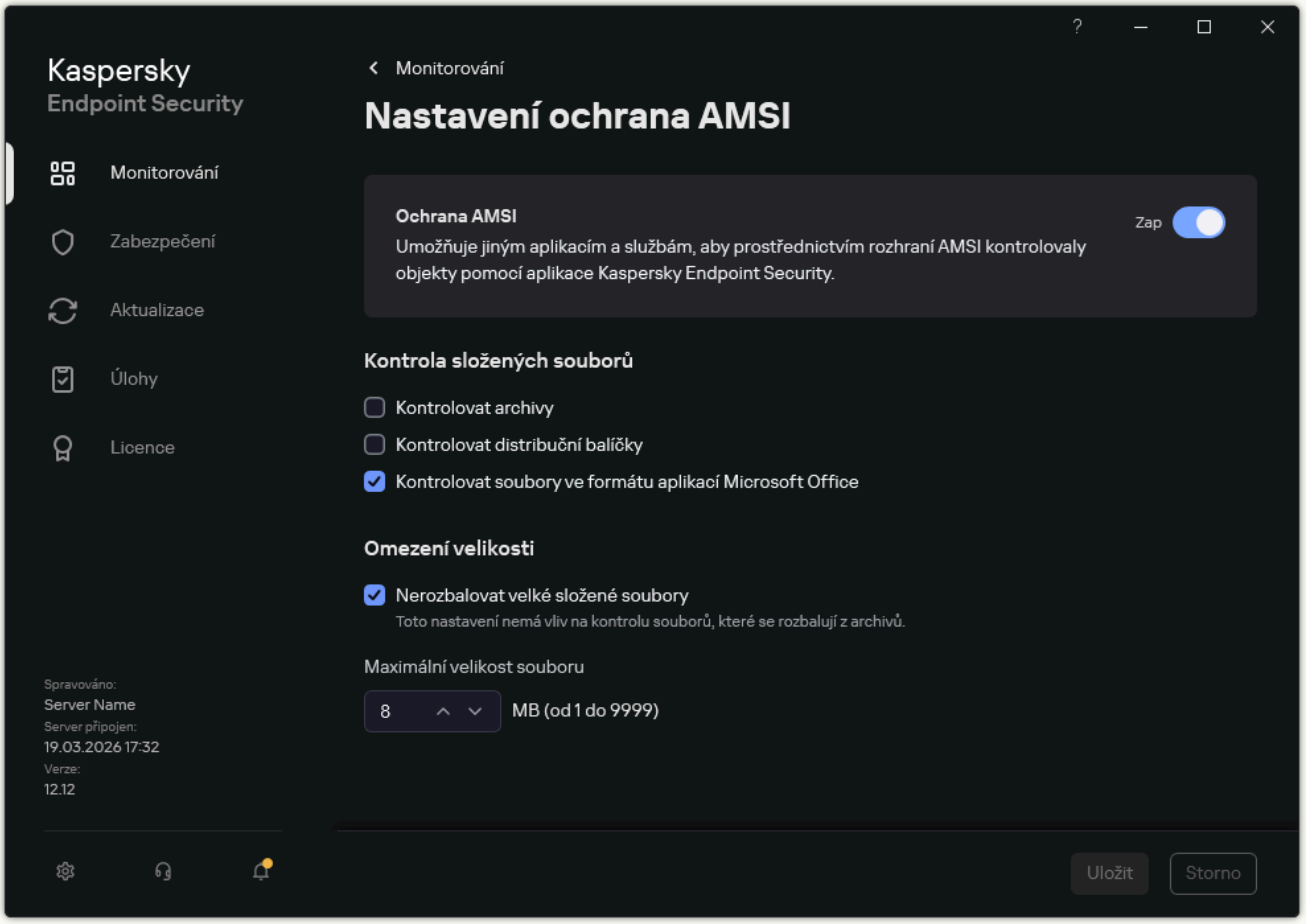
5. Pomocí přepínače **AMSI Protection ENABLED** můžete tuto součást povolit nebo zakázat.

6. Uložte změny. Chcete-li zásady použít v počítačích, zavřete zámky.

Jak povolit nebo zakázat součást Ochrana AMSI v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko.

2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana AMSI**.



Nastavení ochrany AMSI

3. Pomocí přepínače **Ochrana AMSI** můžete tuto součást povolit nebo zakázat.

4. Uložte změny.

Nastavení součásti Ochrana AMSI doporučené odborníky společnosti Kaspersky

Parametr	Hodnota	Popis
Kontrolovat archivy	**Vyp**	Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).
Kontrolovat distribuční balíčky	**Vyp**	Kontrola distribučních balíčků aplikací třetích stran.
Kontrolovat soubory ve formátu aplikací Microsoft Office	**Zap**	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
Nerozbalovat velké složené soubory	**Maximální velikost souboru 8 MB**	Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí. Aplikace kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.

Optimalizace kontroly souborů součástí Ochrana AMSI

Kontrolu souborů můžete optimalizovat: zkrátit dobu trvání kontroly a zvýšit rychlost operací aplikace Kaspersky Endpoint Security. Můžete vybrat složené soubory, které je třeba kontrolovat: archivy, distribuční balíčky nebo soubory v kancelářských formátech. Můžete také omezit velikost složených souborů, které se mají kontrolovat. Součást Ochrana AMSI nebude rozbalovat velké složené soubory překračující zadanou velikost.

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. Typy kontrolovaných složených souborů můžete omezit a tím kontrolu urychlit.

Jak optimalizovat kontroly souborů součástí Ochrana AMSI v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Nástroj pro kontrolu AMSI**.
4. V bloku **Kontrola složených souborů** zadejte typy složených souborů, které chcete kontrolovat: archivy, distribuční balíček nebo soubory ve formátech sady Office.
5. V bloku **Omezení velikosti** proveďte některou z následujících akcí:
   - Chcete-li zabránit tomu, aby součást Ochrana AMSI rozbalovala velké složené soubory, zaškrtněte políčko **Nerozbalovat velké složené soubory** a zadejte požadovanou hodnotu. 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**.
6. Uložte změny. Chcete-li zásady použít v počítačích, zavřete zámky.

Jak optimalizovat kontrolu souborů součástí Ochrana AMSI ve webové konzole a cloudové konzole

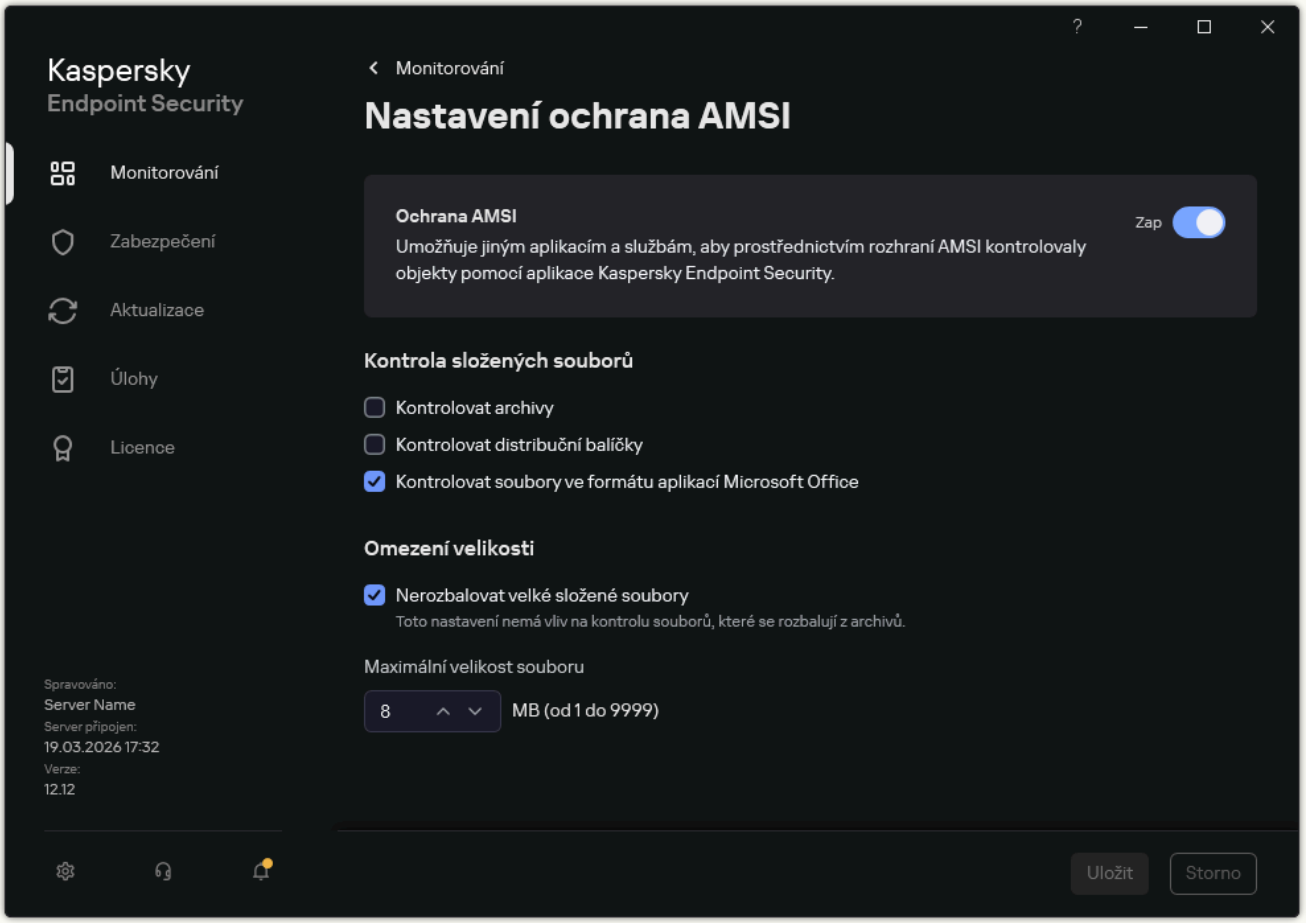
1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **AMSI Protection**.
5. V bloku **Scan of compound files** zadejte typy složených souborů, které chcete kontrolovat: archivy, distribuční balíček nebo soubory ve formátech sady Office.
6. V bloku **Scan optimization** proveďte některou z následujících akcí:
   - Chcete-li zabránit tomu, aby součást Ochrana AMSI rozbalovala velké složené soubory, zaškrtněte políčko **Size limits enabled** a zadejte požadovanou hodnotu. 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 **Size limits enabled**.

   Součást Ochrana AMSI kontroluje velké soubory extrahované z archivů bez ohledu na to, zda je či není zaškrtnuto políčko **Size limits enabled**.
7. Uložte změny. Chcete-li zásady použít v počítačích, zavřete zámky.

Jak optimalizovat kontrolu souborů součástí Ochrana AMSI v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana AMSI**.



Nastavení ochrany AMSI

3. V bloku **Kontrola složených souborů** zadejte typy složených souborů, které chcete kontrolovat: archivy, distribuční balíček nebo soubory ve formátech sady Office.
4. V bloku **Omezení velikosti** proveďte některou z následujících akcí:
   - Chcete-li zabránit tomu, aby součást Ochrana AMSI rozbalovala velké složené soubory, zaškrtněte políčko **Nerozbalovat velké složené soubory** a zadejte požadovanou hodnotu. 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.

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.

Chcete-li používat součást Ochrana před webovými hrozbami, musíte provést počáteční konfiguraci aplikace:

- Pro monitorování provozu HTTPS povolte kontrolu šifrovaných připojení (ve výchozím nastavení povolena).
- Vyberte porty, které aplikace Kaspersky Endpoint Security má monitorovat (ve výchozím nastavení aplikace monitoruje všechny porty).

- Vyberte aplikace, jejichž provoz má aplikace Kaspersky Endpoint Security sledovat. Většina prohlížečů se již nachází v seznamu aplikací doporučených společností Kaspersky. Pokud váš prohlížeč v seznamu chybí, přidejte jej ručně.

- Doporučujeme vložit do webového provozu skript interakce s webovou stránkou (ve výchozím nastavení je vkládání skriptů zakázáno). Tento skript umožňuje evidenci událostí součásti Ochrana před webovými hrozbami pro protokol událostí aplikace, protokol událostí OS a zprávy.

Když se uživatel pokusí otevřít škodlivý nebo phishingový web, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění.

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 použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy 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.

Úroveň zabezpečení můžete nebo konfigurovat vybrat pouze v konzole pro správu nebo místním rozhraní aplikace. Ve webové konzole ani cloudové konzole nemůžete vybírat ani konfigurovat úroveň zabezpečení.

Jak povolit nebo zakázat součást Ochrana před webovými hrozbami v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
4. Pomocí zaškrtávacího políčka **Ochrana před webovými hrozbami** můžete tuto součást povolit nebo zakázat.
5. Pokud jste součást povolili, v bloku **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 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 **Nastavení** a definujte vlastní nastavení součásti.

     Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Výchozí režim**.
6. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty webového provozu:
   - **Blokovat**. 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.
7. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před webovými hrozbami ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Communication & Web Protection → Web Threat Protection**.

5. Pomocí přepínače **Web Threat Protection ENABLED** můžete tuto součást povolit nebo zakázat.

6. V bloku **Action on threat detection** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty webového provozu:

   - **Block**. 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.

   - **Allow, inform, or prompt for action (depends on OS)**. 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.

7. Pokud je potřeba, vytvořte seznam důvěryhodných webových adres.

8. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před webovými hrozbami

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **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 bloku **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 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**.

5. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty webového provozu:

   - **Blokovat**. 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.

6. Uložte změny.

Nastavení ochrany před webovými hrozbami doporučená odborníky společnosti Kaspersky (doporučená úroveň zabezpečení)

Parametr	Hodnota	Popis
Porovnat webovou adresu s databází škodlivých webových adres	**Zap**	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 webovou adresu s databází phishingových webových adres	**Zap**	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)	**Zap**	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**	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.

Konfigurace způsobů zjišťování škodlivých webových adres

Ochrana před webovými hrozbami zjišťuje škodlivé webové adresy pomocí antivirových databází, služby Kaspersky Security Network a heuristické analýzy.

Způsoby zjišťování škodlivých webových adres můžete vybrat pouze v konzole pro správu nebo místním rozhraní aplikace. Ve webové konzole ani cloudové konzole nemůžete vybírat způsoby zjišťování škodlivých webových adres. Výchozí možností je kontrola webových adres oproti databázi škodlivých adres pomocí heuristické analýzy (střední kontrola).

Kontrola pomocí databáze škodlivých adres

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 Security 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 je zakázána kontrola šifrovaných připojení, kontroluje aplikace Kaspersky Endpoint Security v databázích škodlivých webových adres, i když je síťový provoz přenášen přes šifrované připojení.

Jak povolit nebo zakázat kontrolu webových adres oproti databázi škodlivých webových adres pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, v bloku **Metody kontroly**, zaškrtnutím políčka **Porovnat webovou adresu s databází škodlivých webových adres** nebo zrušením jeho zaškrtnutí povolte nebo zakažte kontrolu adres oproti databázi škodlivých webových adres.
6. Uložte změny.

Jak povolit nebo zakázat kontrolu adres oproti databázi škodlivých adres v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Metody kontroly**, zaškrtnutím políčka **Porovnat webovou adresu s databází škodlivých webových adres** nebo zrušením jeho zaškrtnutí povolte nebo zakažte kontrolu adres oproti databázi škodlivých webových adres.

5. Uložte změny.

Heuristická analýza

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.

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.

Jak povolit nebo zakázat používání heuristické analýzy v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. Pokud chcete, aby aplikace při kontrole webového provozu na přítomnost virů a dalšího malwaru používala heuristickou analýzu, v okně, které se otevře, v bloku **Metody kontroly** zaškrtněte políčko **Použít heuristickou analýzu**.
6. Pomocí posuvníku nastavte úroveň heuristické analýzy: **lehká kontrola**, **střední kontrola** nebo **hloubková kontrola**.

   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.
7. Uložte změny.

Jak povolit nebo zakázat používání heuristické analýzy v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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**.

   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.
5. Uložte změny.

Anti-Phishing

Ochrana před webovými hrozbami u odkazů kontroluje, zda nepatří k phishingovým webovým adresám. To pomáhá předcházet *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 messengery, 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.

Součást Anti-Phishing můžete konfigurovat pouze v konzole pro správu (MMC) nebo v místním rozhraní aplikace. Součást Anti-Phishing nelze konfigurovat ve webové konzole ani cloudové konzole. Ve výchozím nastavení je povolena součást Anti-Phishing s heuristickou analýzou.

Jak povolit nebo zakázat součást Anti-Phishing v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, v bloku **Nastavení součásti Anti-Phishing** zaškrtnutím políčka **Porovnat webovou adresu s databází phishingových webových adres** nebo zrušením jeho zaškrtnutí povolíte nebo zakážete součást Anti-Phishing.

   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.
6. Pokud chcete, aby aplikace při kontrole webového provozu na přítomnost phishingových odkazů používala heuristickou analýzu, zaškrtněte políčko **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.

   Ke kontrole odkazů můžete kromě antivirové databáze a heuristické analýzy použít databáze reputace služby Kaspersky Security Network.
7. Uložte změny.

Jak povolit nebo zakázat součást Anti-Phishing v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Pokud chcete, aby součást Ochrana před webovými hrozbami kontrolovala odkazy v databázích phishingových webových adres, zaškrtněte v bloku **Anti-Phishing** políčko **Porovnat webovou adresu s databází phishingových webových adres**. 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.
5. Pokud chcete, aby aplikace při kontrole webového provozu na přítomnost phishingových odkazů používala heuristickou analýzu, zaškrtněte políčko **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.

   Ke kontrole odkazů můžete kromě antivirové databáze a heuristické analýzy použít databáze reputace služby Kaspersky Security Network.
6. Uložte změny.

Vytvoření seznamu důvěryhodných webových adres

Kromě škodlivých a phishingových webů může Ochrana před webovými hrozbami blokovat i další weby. Ochrana před webovými hrozbami například blokuje provoz HTTP, který nesplňuje standardy RFC. 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 známého webu.

Adresa URL může být adresou webu nebo určité webové stránky.

Změnu seznamu důvěryhodných webových adres v zásadě mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak přidat důvěryhodnou webovou adresu pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, vyberte část **Důvěryhodné webové adresy**.
6. Zaškrtněte políčko **Nekontrolovat webový provoz z důvěryhodných webových adres**.

   Pokud je vybrána tato možnost, 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.
7. Vytvořte seznam adres URL / webových stránek s důvěryhodným obsahem.

   Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.

   Můžete také importovat seznam důvěryhodných webových adres ze souboru XML.
8. Uložte změny.

Jak přidat důvěryhodnou webovou adresu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection → Web Threat Protection**.
5. Klikněte na tlačítko **Trusted web addresses**.
6. Vytvořte seznam adres URL / webových stránek s důvěryhodným obsahem.

   Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.

   Můžete také importovat seznam důvěryhodných webových adres ze souboru XML.
7. Uložte změny.

Jak přidat důvěryhodnou webovou adresu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před webovými hrozbami**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. Zaškrtněte políčko **Nekontrolovat webový provoz z důvěryhodných adres URL**.

   Pokud je vybrána tato možnost, 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.

   Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.

   Můžete také importovat seznam důvěryhodných webových adres ze souboru XML.
6. Uložte změny.

V důsledku toho Ochrana před webovými hrozbami nekontroluje provoz u důvěryhodných webových adres. Uživatel může vždy otevřít důvěryhodný web a stáhnout z něj soubor. Pokud se vám nepodařilo získat přístup k webu, zkontrolujte nastavení součástí Kontrola šifrovaného připojení, Kontrola webu a Monitorování síťových portů. Pokud aplikace Kaspersky Endpoint Security zjistí, že je soubor stažený z důvěryhodného webu škodlivý, můžete přidat tento soubor do výjimek.

Můžete také vytvořit obecný seznam výjimek pro šifrovaná připojení. V tomto případě Kaspersky Endpoint Security nekontroluje HTTPS provoz důvěryhodných webových adres, když součásti Ochrana před webovými hrozbami, Ochrana před hrozbami v poště a Kontrola webu vykonávají svoji práci.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před webovými hrozbami**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, vyberte část **Důvěryhodné webové adresy**.
6. 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. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam důvěryhodných adres do souboru XML.
7. 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. Otevřete soubor.
      Pokud počítač již seznam důvěryhodných adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.
8. Uložte změny.

Jak exportovat a importovat seznam důvěryhodných webových adres ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection** → **Web Threat Protection**.
5. Postup exportu seznamu výjimek v bloku **Rules list**:
   a. Vyberte důvěryhodné webové adresy, které chcete exportovat.
   b. Klikněte na tlačítko → **Export**.

Aplikace Kaspersky Endpoint Security exportuje seznam důvěryhodných webových adres do souboru JSON ve výchozí složce pro stahování.

6. Postup exportu seznamu výjimek v bloku **Rules list**:

   a. Klikněte na tlačítko → **Import**.

   V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam důvěryhodných adres.

   b. Otevřete soubor.

   Pokud počítač již seznam důvěryhodných adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.

7. Uložte změny.

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 poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Ochrana před hrozbami v poště může kontrolovat příchozí i odchozí zprávy. Aplikace podporuje POP3, SMTP, IMAP a NNTP v následujících poštovních klientech:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pokud chcete kontrolovat provoz v poštovních klientech Mozilla Thunderbird, MyOffice Mail a R7-Office Organizer, musíte přidat certifikát Kaspersky do úložiště certifikátů a vybrat vlastní úložiště certifikátů.

Ochrana před hrozbami v poště nepodporuje jiné protokoly a poštovní klienty.

Ochrana před hrozbami v poště nemusí být vždy schopna získat přístup ke zprávám na *úrovni protokolu* (například při použití řešení Microsoft Exchange). Z tohoto důvodu Ochrana před hrozbami pošty zahrnuje rozšíření pro Microsoft Office Outlook. Rozšíření umožňuje kontrolu zpráv na *úrovni poštovního klienta*. Rozšíření Ochrana před hrozbami v poště podporuje 32bitové verze aplikace Outlook 2010, 2013, 2016, 2019, 2021, 2024 a 365. V počítačích s architekturou ARM podporuje rozšíření Ochrana před hrozbami v poště 32bitové verze aplikace Outlook 2016, Outlook 2021, Outlook 2024 a Outlook 365 pro Arm64.

Součást Ochrana před hrozbami v poště nekontroluje zprávy, pokud je poštovní klient otevřen v prohlížeči.

Když je v příloze zjištěn škodlivý soubor, aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

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 použít různé skupiny nastavení. Tyto sady nastavení, které jsou uloženy 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.

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.

Jak povolit nebo zakázat součást Ochrana před hrozbami v poště v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před hrozbami v poště**.

4. Pomocí zaškrtávacího políčka **Ochrana před hrozbami v poště** můžete tuto součást povolit nebo zakázat.

5. Pokud jste součást povolili, v bloku **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 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 **Nastavení** a definujte vlastní nastavení součásti.

     Hodnoty přednastavených úrovní zabezpečení můžete obnovit kliknutím na tlačítko **Výchozí režim**.

6. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:

   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

   - **Blokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Ochrana před hrozbami v poště ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Communication & Web Protection → Mail Threat Protection**.

5. Pomocí přepínače **Mail Threat Protection ENABLED** můžete tuto součást povolit nebo zakázat.

6. V bloku **Action on threat detection** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:

   - **Disinfect, delete if disinfection fails**. Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

   - **Disinfect, block if disinfection fails**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

   - **Block**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

7. V případě potřeby upravte pokročilé nastavení ochrany před hrozbami v poště.

8. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před hrozbami v poště v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **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 bloku **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 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**.

5. V bloku **Akce při zjištění hrozby** vyberte akci, kterou má aplikace Kaspersky Endpoint Security provést se škodlivými objekty:

   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit**. Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

   - **Blokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

6. 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	**Zap**	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 Cached Exchange Mode. Podrobnější informace o režimu serveru Exchange s mezipamětí a o doporučeních k jeho použití najdete ve znalostní bázi Microsoft Knowledge Base.

Kontrolovat připojené archivy	**Zap**	Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).
Kontrolovat přiložené soubory ve formátu aplikací Microsoft Office	**Zap**	Aplikace bude kontrolovat soubory aplikace Microsoft Office (DOC, DOCX, XLS, PPT a další přípony společnosti Microsoft). Soubory formátu Office zahrnují také objekty OLE. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
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; a pokud se dezinfekce nezdaří, tak odstranit**	Pokud je v příchozí nebo odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před hrozbami v poště**.
3. V bloku **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 tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.
   - **Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.
   - **Blokovat**. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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 bloku **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**.

     Pokud používáte jiného poštovního klienta než Microsoft Office Outlook, součást Ochrana před hrozbami v poště nekontroluje zprávy přenášené prostřednictvím protokolů POP3, SMTP, NNTP a IMAP, když 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před hrozbami v poště**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
   - **Kontrolovat připojené archivy**. Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).

     Pokud aplikace 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 (od 1 do 9999)**. 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 na kontrolu archivů na N s (od 1 do 9999)**. 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před hrozbami v poště**.
3. Klikněte na tlačítko **Rozšířené nastavení**.
4. V bloku **Filtr příloh** proveďte některou z následujících akcí:
   - **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.
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. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection → Mail Threat Protection**.
5. Postup exportu seznamu rozšíření v bloku **Attachment filter**:
   a. Vyberte rozšíření, která chcete exportovat.
   b. Klikněte na odkaz **Export**.
   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. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam rozšíření do souboru XML.

6. Postup exportu seznamu rozšíření v bloku **Attachment filter**:

   a. Klikněte na odkaz **Import**.

   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam rozšíření.

   c. Otevřete soubor.

   Pokud počítač již seznam rozšíření obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

7. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před hrozbami v poště**.

4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.

5. Tím otevřete okno; v tomto okně vyberte kartu **Filtr příloh**.

6. 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. Uložte soubor.

   Aplikace Kaspersky Endpoint Security exportuje celý seznam rozšíření do souboru XML.

7. 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. Otevřete soubor.

   Pokud počítač již seznam rozšíření obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

8. 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). Rozšíření umožňuje kontrolu zpráv na úrovni poštovního klienta namísto na úrovni protokolu. Kromě zpráv vám rozšíření umožňuje kontrolovat objekty přijaté prostřednictvím rozhraní MAPI z úložišť Microsoft Exchange (například objekty v Kalendáři). Tato kontrola probíhá v poštovním klientovi.

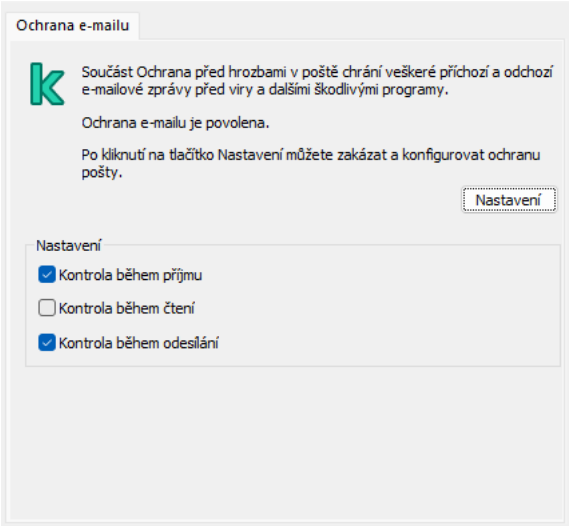
Můžete otevřít nastavení součásti Ochrana před hrozbami v poště z aplikace Outlook a určit, kdy se mají e-maily kontrolovat na přítomnost virů a jiných hrozeb.

Rozšíření Ochrana před hrozbami v poště podporuje 32bitové verze aplikace Outlook 2010, 2013, 2016, 2019, 2021, 2024 a 365.

V počítačích s architekturou ARM podporuje rozšíření Ochrana před hrozbami v poště 32bitové verze aplikace Outlook 2016, Outlook 2021, Outlook 2024 a Outlook 365 pro Arm64.

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 (viz obrázek níže).



Nastavení součásti Ochrana před hrozbami v poště v aplikaci Outlook

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:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před hrozbami v poště**.
4. V bloku **Úroveň zabezpečení** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, v bloku **Možnosti připojení** klikněte na tlačítko **Nastavení**.
6. V okně **Ochrana e-mailu** proveďte jednu z následujících akcí:
   - 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**.
7. Uložte změny.

Kontrola e-mailů v aplikacích Thunderbird, MyOffice a R7-Office

Součást Ochrana před hrozbami v poště v přílohách kontroluje, zda příchozí a odchozí e-maily obsahují viry nebo jiné hrozby. V případě poštovních klientů Mozilla Thunderbird, MyOffice Mail a R7-Office Organizer aplikace získává přístup ke zprávám pouze na adrese *na úrovni protokolu* (POP3, SMTP, IMAP, NNTP).

Pokud chcete kontrolovat provoz v poštovních klientech Mozilla Thunderbird, MyOffice Mail a R7-Office Organizer, musíte přidat certifikát Kaspersky do úložiště certifikátů a vybrat vlastní úložiště certifikátů.

Součást Ochrana před hrozbami v poště nekontroluje zprávy, pokud je poštovní klient otevřen v prohlížeči.

Ochrana před hrozbami v poště v reálném čase

Ochrana před hrozbami v poště může kontrolovat příchozí i odchozí zprávy. 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. Když je v příloze zjištěn škodlivý soubor, aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

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.

Kontrola malwaru v databázích pošty

Úloha *Kontrola malwaru* umožňuje kontrolu souborů ve formátu pošty. Pokud je v souborech těchto poštovních klientů zjištěn škodlivý objekt, Kaspersky Endpoint Security pouze přidá na seznam aktivních hrozeb informace o zjištěných objektech. Aplikace nedezinfikuje ani neodstraňuje infikované soubory v databázích pošty bez ohledu na nastavení úlohy.

Eliminace aktivních hrozeb

Ochrana před hrozbami v poště předchází infekci počítače na úrovni protokolu, ale pokud byl počítač infikován před instalací aplikace Kaspersky Endpoint Security, aplikace může hrozbu zjistit pouze v databázích pošty. Ochrana před hrozbami v poště nezahrnuje součásti, které konkrétně umožňují rozebrat zprávu na části (záhlaví, tělo, přílohy), např. Microsoft Office Outlook. Aplikace proto nemůže zjištěné objekty odstranit ani dezinfikovat. Kaspersky Endpoint Security pouze přidá informace o zjištěných objektech na seznam aktivních hrozeb.

Postup eliminace aktivních hrozeb:

1. Zprávu se zjištěným objektem ručně vyhledejte a odstraňte v rozhraní poštovního klienta.

   Aplikace zobrazuje informace o zjištěném objektu na seznamu aktivních hrozeb.

   Příklad karty zjištěného objektu:

   HEUR:Trojan.PDF.Phish.gen

   Objekt: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox//[From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36][Subj Mail title X] Object.pdf`

2. Proveďte operaci komprimace databáze.

   Po odstranění zprávy v uživatelském rozhraní poštovní klient pouze přidá značku odstranění. Poštovní klient zprávu skutečně odstraní až po komprimaci databáze. Podrobnosti o komprimaci databáze najdete v nápovědě k poštovnímu klientovi (například Mozilla Thunderbird).

3. Spusťte úlohu *Kontrola malwaru* znovu a ujistěte se, že hrozba již není přítomná.

Ochrana před síťovými hrozbami

Součást *Ochrana před síťovými hrozbami* (také nazývaná Intrusion Detection System, IDS) monitoruje příchozí síťový provoz a sleduje aktivitu charakteristickou pro síťové útoky. Pokud aplikace 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. 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. Kaspersky Endpoint Security u příchozího síťového provozu monitoruje aktivitu charakteristickou pro síťové útoky a tyto útoky blokuje.

Jak povolit nebo zakázat součást Ochrana před síťovými hrozbami v konzole pro správu (MMC)

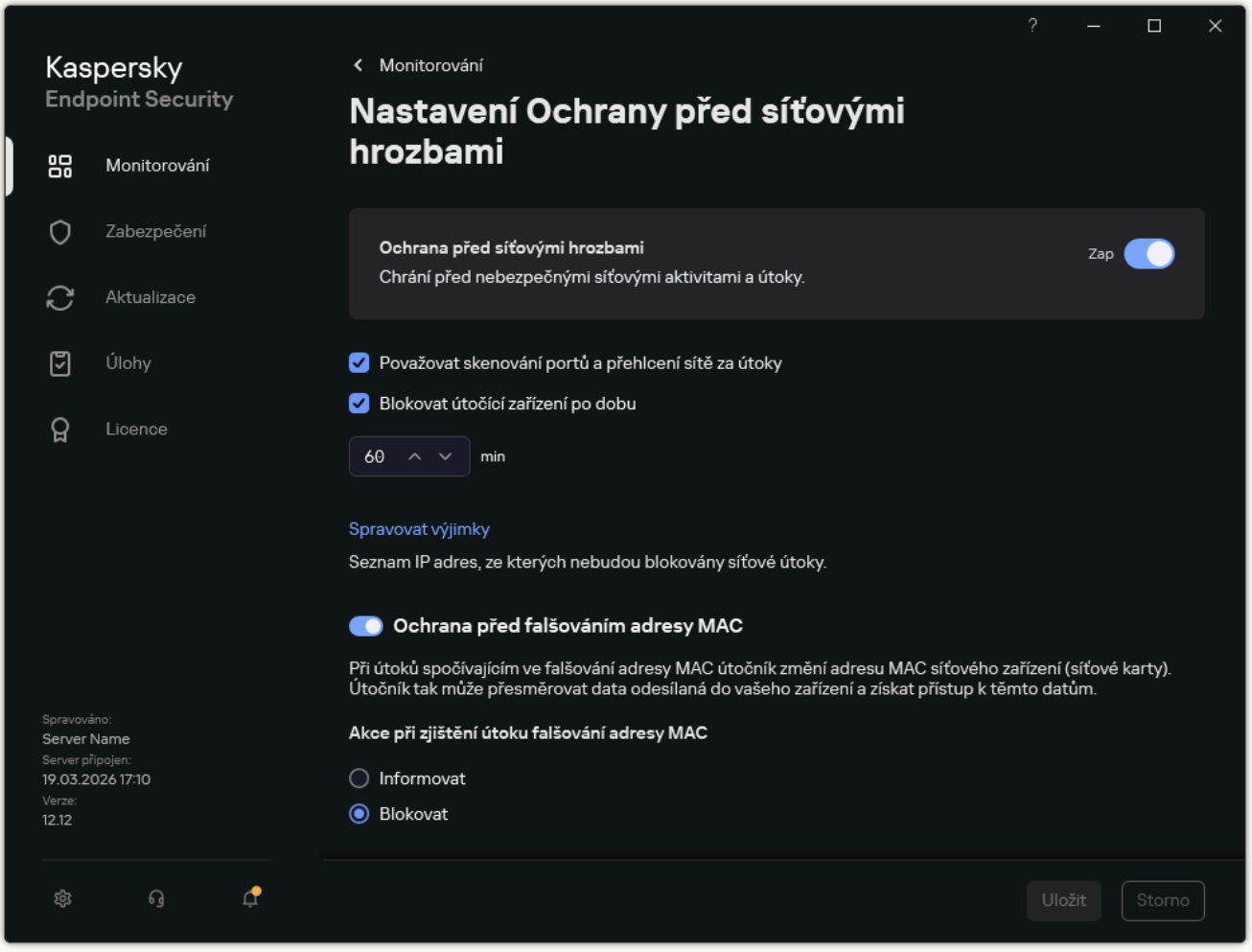
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před síťovými hrozbami**.
4. Pomocí zaškrtávacího políčka **Ochrana před síťovými hrozbami** můžete tuto součást povolit nebo zakázat.
5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Ochrana před síťovými hrozbami ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection** → **Network Threat Protection**.
5. Pomocí přepínače **Network Threat Protection ENABLED** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

Jak povolit nebo zakázat součást Ochrana před síťovými hrozbami v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Ochrana před síťovými hrozbami**.



Nastavení Ochrany před síťovými hrozbami

3. Pomocí přepínače **Ochrana před síťovými hrozbami** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Blokování útočícího počítače

Pokud je povolena součást Ochrana před síťovými hrozbami, Kaspersky Endpoint Security automaticky blokuje síťové hrozby. Kromě toho může aplikace zablokovat útočící počítač a omezit odesílání síťových paketů na určitou dobu. Ve výchozím nastavení Kaspersky Endpoint Security blokuje počítač na jednu hodinu.

Jak zablokovat útočící počítač v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.
4. V části **Nastavení Ochrany před síťovými hrozbami** zaškrtněte políčko **Blokovat útočící zařízení po dobu N min**.

   Pokud je tato možnost povolena, 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. Minimální doba, kterou musí útočící počítač strávit na seznamu blokovaných počítačů, je jedna minuta. Maximální doba je 999 minut.
5. Nastavte jinou dobu blokování pro útočící počítač v poli napravo od zaškrtávacího políčka **Blokovat útočící zařízení po dobu N min**.
6. Uložte změny.

Jak zablokovat útočící počítač ve webové konzole a cloudové konzole

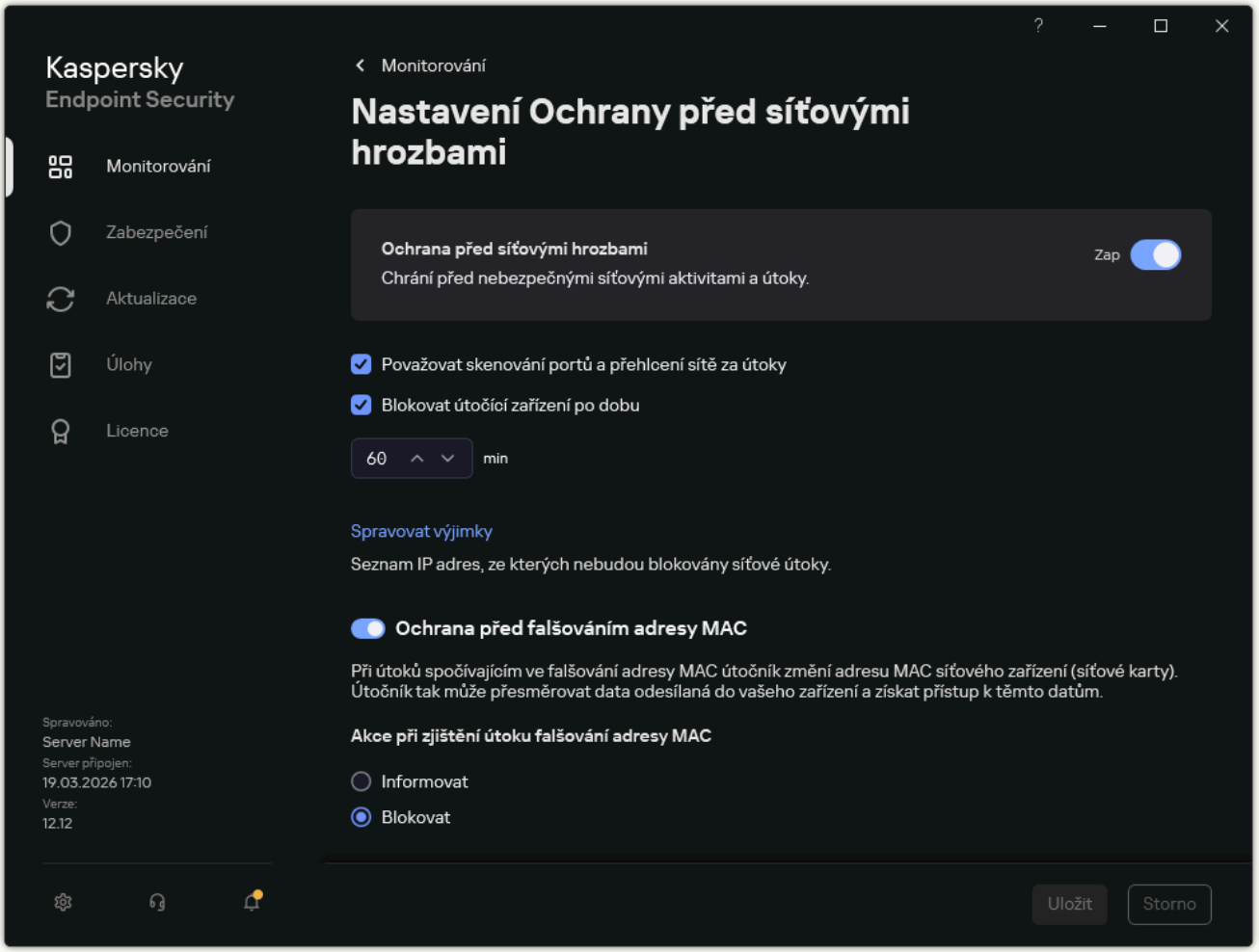
1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection → Network Threat Protection**.
5. V bloku **Action on threat detection** zaškrtněte políčko **Block attack and attacking device for (min)**.

   Pokud je tato možnost povolena, 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. Minimální doba, kterou musí útočící počítač strávit na seznamu blokovaných počítačů, je jedna minuta. Maximální doba je 999 minut.
6. Změňte dobu blokování útočícího počítače.
7. Uložte změny.

Jak zablokovat útočící počítač v uživatelském rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.



Nastavení Ochrany před síťovými hrozbami

3. Zapněte přepínač **Blokovat útočící zařízení po dobu N min**.

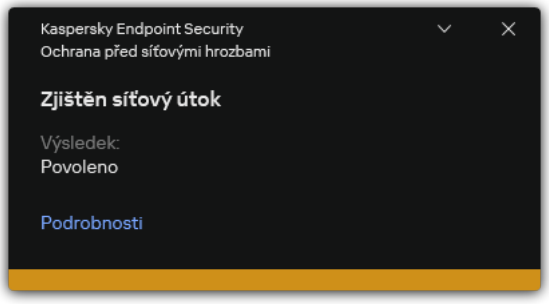
   Pokud je tato možnost povolena, přidá součást Ochrana před síťovými hrozbami útočící počítač do seznamu blokovaných počítačů. Znamená to, že součást Ochrana před síťovými hrozbami bude síťové propojení s útočícím počítačem blokovat po zadanou dobu od prvního pokusu o síťový útok. Takové blokování automaticky chrání počítač uživatele před možnými budoucími síťovými útoky ze stejné adresy. Minimální doba, kterou musí útočící počítač strávit na seznamu blokovaných počítačů, je jedna minuta. Maximální doba je 999 minut.

4. Nastavte jinou dobu blokování pro útočící počítač v poli pod přepínačem **Blokovat útočící zařízení po dobu N min**.

5. Uložte změny.

Pokud aplikace Kaspersky Endpoint Security zjistí pokus o útok na síť v počítači uživatele, zablokuje všechna síťová připojení s útočícím počítačem. Kaspersky Endpoint Security vytváří události *Network attack detected*. Událost obsahuje informace o útočícím počítači: IP a MAC adresy.

Adresu MAC útočícího počítače můžete zobrazit v uživatelském rozhraní aplikace nebo v konzole aplikace Kaspersky Security Center Linux verze 15.1 nebo novější.



Upozornění na zjištění síťového útoku

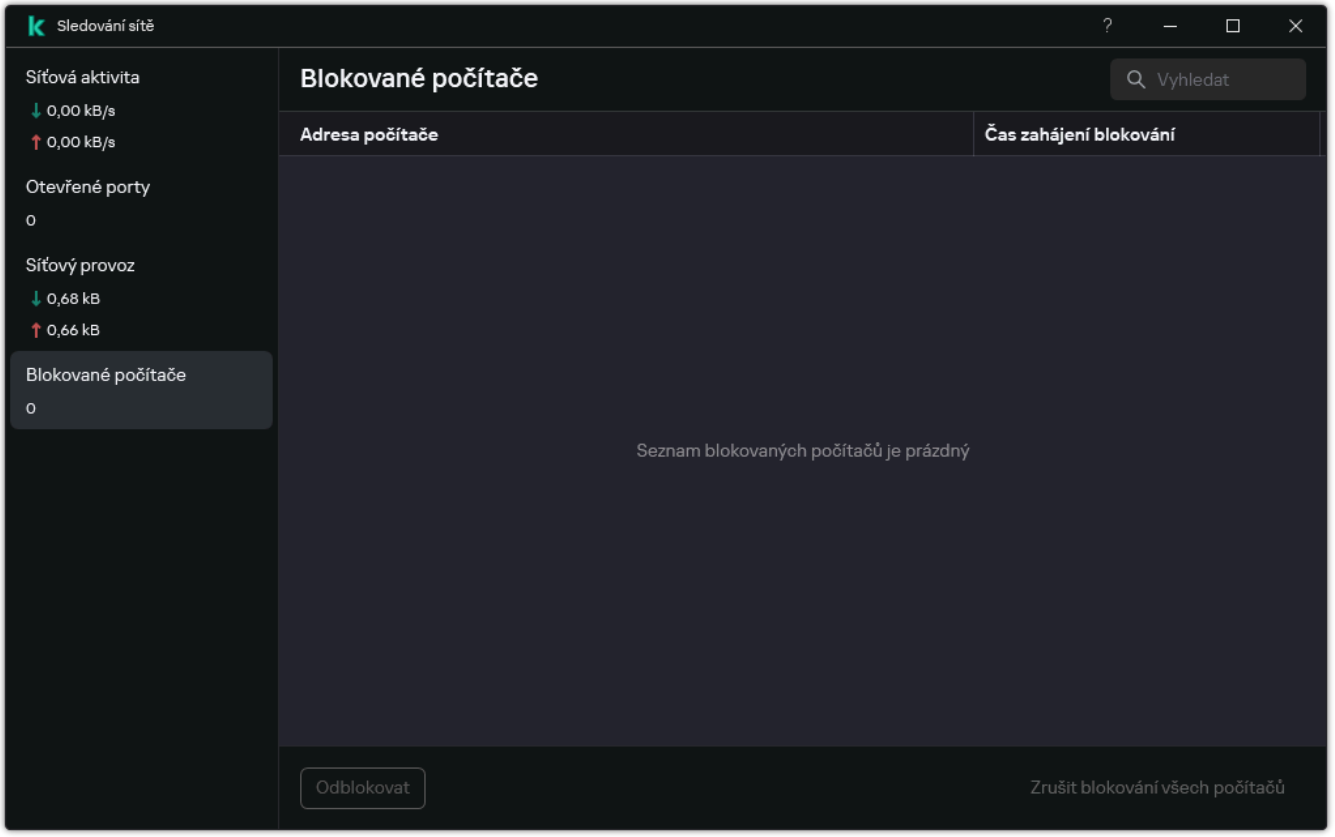
Kaspersky Endpoint Security odblokuje počítač, jakmile vyprší určený čas. Konzola aplikace Kaspersky Security Center neposkytuje jiné nástroje pro sledování zablokovaných počítačů než události *Network attack detected* ve zprávě. Seznam blokovaných počítačů můžete zobrazit pouze v rozhraní aplikace. Tuto funkci zajišťuje nástroj *Sledování sítě*. K odblokování počítače můžete také použít nástroj Sledování sítě.

Postup odblokování počítače:

1. V hlavním okně aplikace v části **Monitorování** klikněte na dlaždici **Sledování sítě**.
2. Přejděte na kartu **Blokované počítače**.
   Otevře se seznam blokovaných počítačů (viz obrázek níže).

   Aplikace Kaspersky Endpoint Security vymaže seznam bloků při svém restartu a při změně nastavení součásti Ochrana před síťovými hrozbami.

3. Vyberte počítač, který chcete odblokovat, a klikněte na možnost **Odblokovat**.



Seznam blokovaných počítačů

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. Můžete také vybrat protokol a port, které se používají pro komunikaci, a povolit specifické síťové aktivity.

Do aplikace Kaspersky Endpoint Security 12.2 byla přidána možnost vybrat protokoly a porty pro výjimky. Ujistěte se, že jsou aplikace a modul plug-in pro správu aktualizovány na verzi 12.2 nebo novější. Pokud používáte dřívější verzi aplikace nebo modul plug-in pro správu, může aplikace Kaspersky Endpoint Security povolit síťové aktivity pouze podle IP adresy.

Změnu seznamu výjimek z blokování mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak nakonfigurovat adresy výjimek z blokování v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

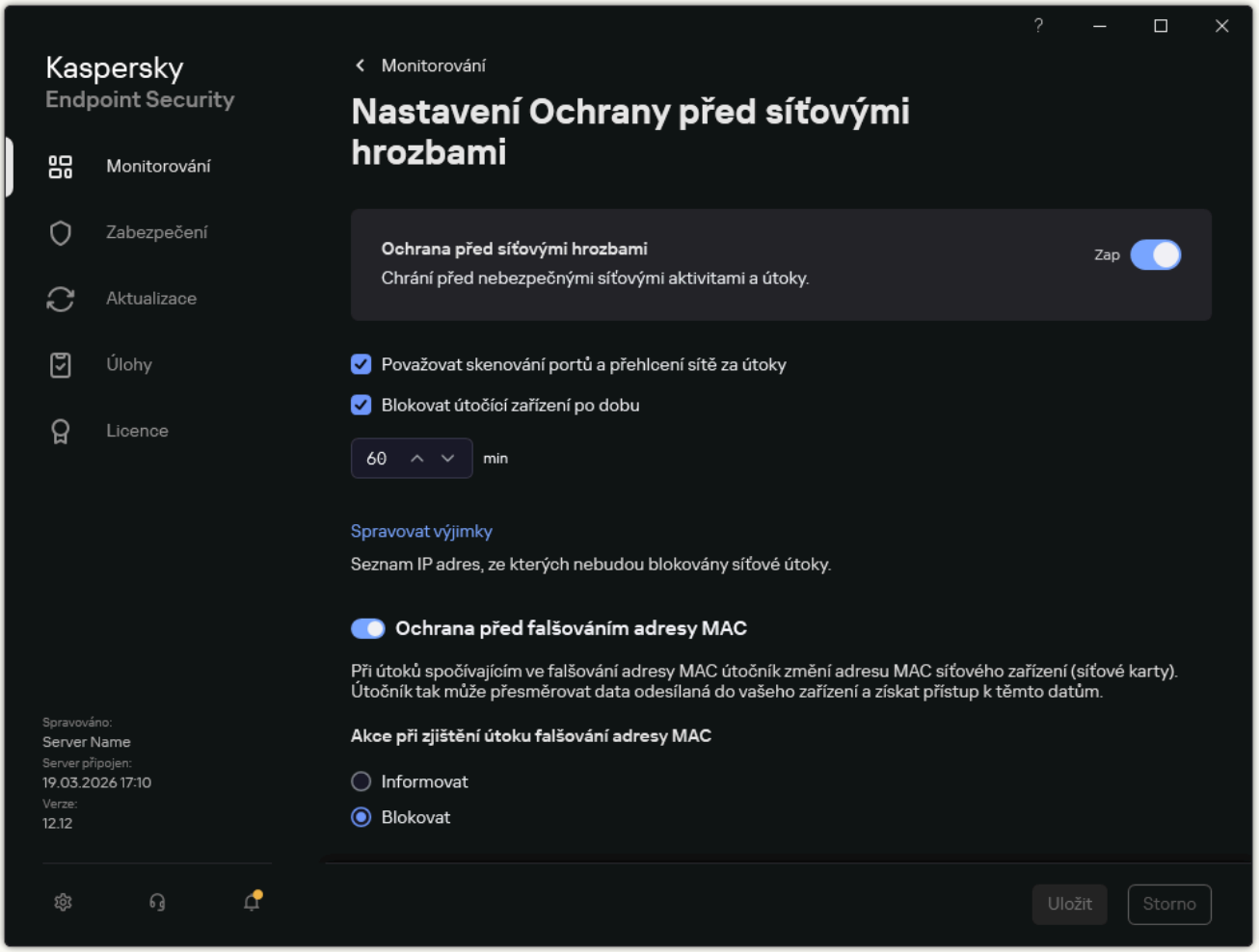
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.
4. V bloku **Nastavení Ochrany před síťovými hrozbami** klikněte na tlačítko **Výjimky**.
5. V okně, které se otevře, klikněte na tlačítko **Přidat**.
6. Zadejte IP adresu počítače, ze kterého nemají být blokovány síťové útoky.
   V případě potřeby vyberte protokol a porty, přes které jsou data přenášena.
7. Uložte změny.

Jak nakonfigurovat adresy výjimek z blokování ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection → Network Threat Protection**.
5. V pravé části okna klikněte na odkaz **Trusted IP addresses**.
6. V okně, které se otevře, klikněte na tlačítko **Add**.
7. Zadejte IP adresu počítače, ze kterého nemají být blokovány síťové útoky.
   V případě potřeby vyberte protokol a porty, přes které jsou data přenášena.
8. Uložte změny.

Jak nakonfigurovat adresy výjimek z blokování v uživatelském rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.



Nastavení Ochrany před síťovými hrozbami

3. Klikněte na odkaz **Spravovat výjimky**.
4. V okně, které se otevře, klikněte na tlačítko **Přidat**.
5. Zadejte IP adresu počítače, ze kterého nemají být blokovány síťové útoky.
   V případě potřeby vyberte protokol a porty, přes které jsou data přenášena.
6. Uložte změny.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami** → **Ochrana před síťovými hrozbami**.
4. V bloku **Nastavení Ochrany před síťovými hrozbami** klikněte na tlačítko **Výjimky**.
5. 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 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. Uložte soubor.

Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.

6. 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. Otevřete soubor.

Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

7. Uložte změny.

Jak exportovat a importovat seznam výjimek ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection** → **Network Threat Protection**.
5. V pravé části okna klikněte na odkaz **Trusted IP addresses**.
   Otevře se seznam výjimek.
6. Postup exportu seznamu pravidel:

a. Vyberte výjimky, které chcete exportovat.

b. Klikněte na tlačítko → **Export**.

Aplikace Kaspersky Endpoint Security exportuje seznam výjimek do souboru JSON ve výchozí složce pro stahování.

7. Postup importu seznamu výjimek:

a. Klikněte na tlačítko → **Import**.

V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam výjimek.

b. Otevřete soubor.

Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru JSON přidá nové položky.

8. Uložte změny.

Konfigurace součásti Ochrana před síťovými hrozbami 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.

Nedoporučujeme povolovat ochranu před falšováním adresy MAC na virtuálních počítačích v infrastruktuře Microsoft Hyper-V. Vzhledem ke specifikům platformy Microsoft Hyper-V může aplikace Kaspersky Industrial CyberSecurity for Nodes zablokovat hypervizor kvůli falešně pozitivním výsledkům.

Jak nakonfigurovat součást Ochrana před síťovými hrozbami podle typu v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.
4. Chcete-li povolit nebo zakázat detekci těchto útoků, použijte zaškrtávací políčko **Považovat skenování portů a přehlcení sítě za útoky**.

   Jestliže je tato funkce povolena, sleduje aplikace Kaspersky Endpoint Security síťový provoz z hlediska skenování portů a zahlcení sítě. Pokud je zjištěno takové chování, aplikace upozorní uživatele a odešle odpovídající událost do aplikace Kaspersky Security Center. Aplikace poskytuje informace o počítači, který tyto požadavky provádí. Tyto informace jsou nezbytné pro včasnou reakci. Aplikace Kaspersky Endpoint Security ale neblokuje počítač, který požadavky odesílá, protože takový provoz může být v podnikové síti běžný.
5. V bloku **Režim fungování ochrany proti falšování adres MAC** vyberte některou z následujících možností:
   - **Nesledovat falšování adres MAC**
   - **Informovat**
   - **Blokovat**.
6. Uložte změny.

Jak nakonfigurovat součást Ochrana před síťovými hrozbami podle typu ve webové konzole a cloudové konzole

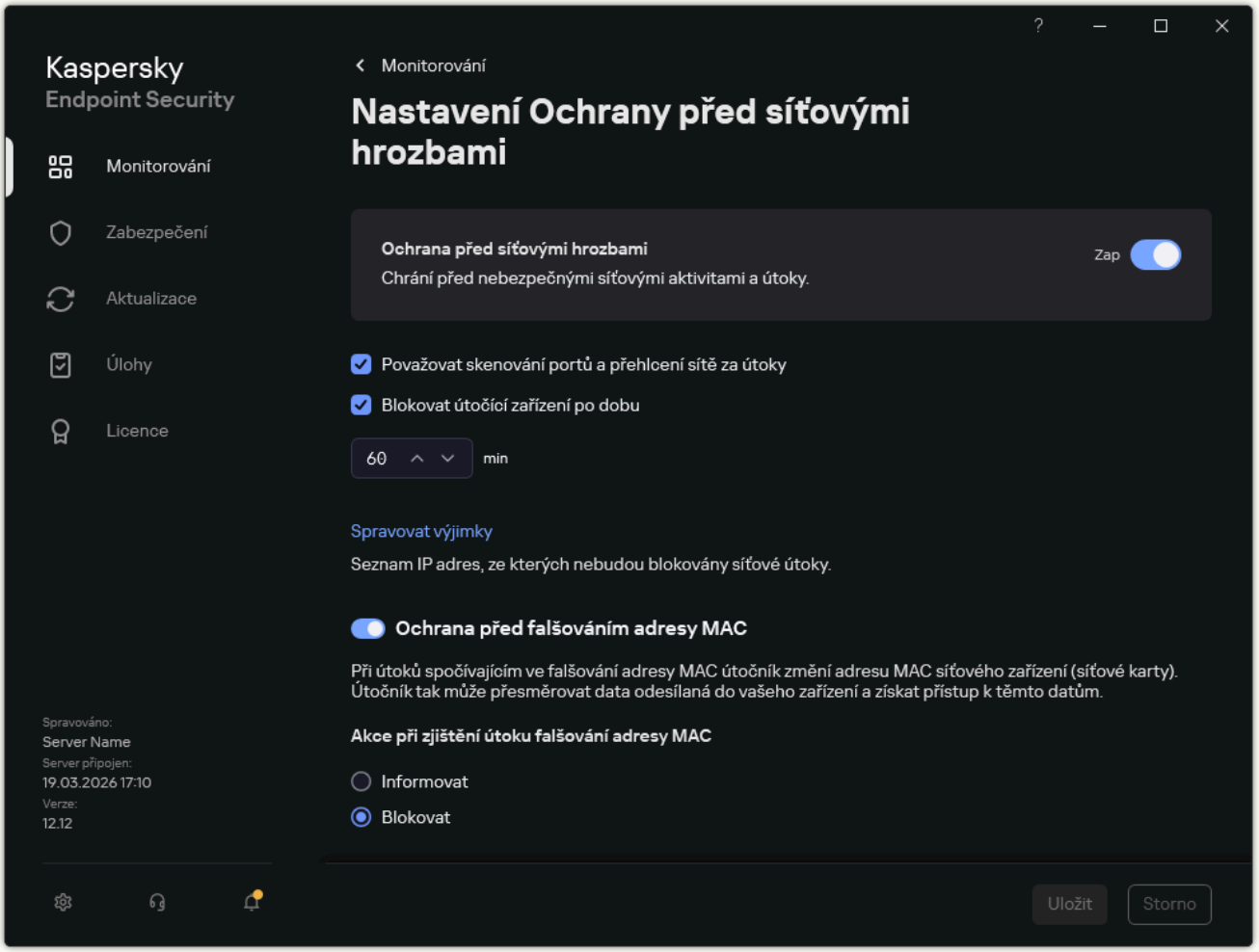
1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection → Network Threat Protection**.
5. Chcete-li povolit nebo zakázat detekci těchto útoků, použijte zaškrtávací políčko **Treat port scanning and network flooding as attacks**.

   Jestliže je tato funkce povolena, sleduje aplikace Kaspersky Endpoint Security síťový provoz z hlediska skenování portů a zahlcení sítě. Pokud je zjištěno takové chování, aplikace upozorní uživatele a odešle odpovídající událost do aplikace Kaspersky Security Center. Aplikace poskytuje informace o počítači, který tyto požadavky provádí. Tyto informace jsou nezbytné pro včasnou reakci. Aplikace Kaspersky Endpoint Security ale neblokuje počítač, který požadavky odesílá, protože takový provoz může být v podnikové síti běžný.
6. V bloku **MAC Spoofing Protection** vyberte některou z následujících možností:
   - **MAC Spoofing Protection ENABLED**
   - **Inform**
   - **Block**.
7. Uložte změny.

Jak nakonfigurovat součást Ochrana před síťovými hrozbami podle typu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**.



Nastavení Ochrany před síťovými hrozbami

3. Chcete-li povolit nebo zakázat detekci těchto útoků, použijte přepínač **Považovat skenování portů a přehlcení sítě za útoky**.

   Jestliže je tato funkce povolena, sleduje aplikace Kaspersky Endpoint Security síťový provoz z hlediska skenování portů a zahlcení sítě. Pokud je zjištěno takové chování, aplikace upozorní uživatele a odešle odpovídající událost do aplikace Kaspersky Security Center. Aplikace poskytuje informace o počítači, který tyto požadavky provádí. Tyto informace jsou nezbytné pro včasnou reakci. Aplikace Kaspersky Endpoint Security ale neblokuje počítač, který požadavky odesílá, protože takový provoz může být v podnikové síti běžný.

4. Chcete-li povolit nebo zakázat detekci těchto útoků, použijte přepínač **Ochrana před falšováním adresy MAC**.

5. V bloku **Akce při zjištění útoku falšování adresy MAC** vyberte některou z následujících možností:

   - **Informovat**.
   - **Blokovat**.

6. Uložte změny.

Brána firewall

Součást 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 součást Network Agent. Brána firewall automaticky vytváří pravidla sítě požadovaná pro fungování aplikace a Network Agent. 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, najdete 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 aplikací*. 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 zabezpečení: *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 důvěryhodnosti *Vysoké omezení* 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.

Síťová pravidla pro aplikace fungují určitým způsobem. Síťové pravidlo pro aplikace zahrnuje pravidla přístupu na základě stavu sítě: *Veřejná síť*, *Místní síť*, *Důvěryhodná síť*. Například aplikace ve skupině důvěryhodnosti *Vysoké omezení* 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.

Typy síťového připojení

Brána firewall umožňuje řídit síťovou aktivitu v závislosti na typu síťového připojení. Aplikace Kaspersky Endpoint Security přijímá typ síťového připojení z operačního systému počítače. Typ síťového připojení v operačním systému nastavuje uživatel při nastavování připojení. Typ síťového připojení můžete změnit v nastavení aplikace Kaspersky Endpoint Security. Brána firewall bude sledovat aktivitu sítě v závislosti na typu sítě zadaného v nastavení aplikace Kaspersky Endpoint Security, a ne v operačním systému.

K dispozici jsou následující typy 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.

  Brána firewall ve výchozím nastavení přiřadí internetu typ *Veřejná síť*. Typ 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.

Jak povolit nebo zakázat bránu firewall v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte možnosti **Základní ochrana před hrozbami → Brána firewall**.
4. Pomocí zaškrtávacího políčka **Brána firewall** můžete tuto součást povolit nebo zakázat.
5. Uložte změny.

Jak povolit nebo zakázat bránu firewall ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Vyberte možnosti **Communication & Web Protection → Firewall**.
5. Pomocí přepínače **Firewall ENABLED** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

Jak povolit nebo zakázat bránu firewall v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.
3. Pomocí přepínače **Brána firewall** můžete tuto součást povolit nebo zakázat.
4. Uložte změny.

Pokud je brána firewall povolena, kontroluje aplikace Kaspersky Endpoint Security síťovou aktivitu a blokuje neoprávněná síťová připojení k vašemu počítači a také blokuje neoprávněnou síťovou aktivitu aplikací ve vašem počítači. Síťovou aktivitu kontroluje také součást Ochrana před síťovými hrozbami. Součást Ochrana před síťovými hrozbami (také nazývaná Systém detekce narušení, IDS) monitoruje příchozí síťový provoz a sleduje aktivitu charakteristickou pro síťové útoky.

Aplikace Kaspersky Endpoint Security zaznamenává do protokolu ve svých zprávách události síťových útoků bez ohledu na nastavení brány firewall. I když brána firewall zablokuje síťové připojení pomocí pravidel a zabrání tak síťovému útoku, součást Ochrana před síťovými hrozbami registruje události síťových útoků. Je to nutné pro generování statistických informací o síťových útocích na počítače ve vaší organizaci.

Změna typu připojení k síti

Brána firewall ve výchozím nastavení přiřadí internetu typ *Veřejná síť*. Typ v případě internetu nelze změnit.

Postup změny typu připojení k síti:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.

3. Klikněte na tlačítko **Dostupné sítě**.

4. Vyberte připojení k síti, jehož typ chcete změnit.

5. Ve sloupci **Typ sítě** vyberte typ 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

Brána firewall filtruje veškerou síťovou aktivitu v počítači v souladu s pravidly síťových paketů. Pravidla síťových paketů obsahují podmínky (například směr, protokol), které brána firewall vztahuje ke kontrole síťových připojení počítače. Pravidla síťových paketů také určují akci, kterou brána firewall provede s připojením, které odpovídá pravidlu (povolí nebo zablokuje připojení).

Doporučení pro vytváření pravidel síťových paketů

Pro filtrování síťové aktivity můžete určit IP adresu nebo rozsah IP adres. Můžete také určit název DNS, ale doporučujeme použití IP adres a rozsahů IP adres. Použití názvů DNS v názvech síťových paketů může být nebezpečné, protože vlastník serveru DNS může měnit parametry záznamu DNS. Útočník se zlými úmysly může také falšovat zprávy DNS a obcházet pravidla brány firewall.

Síťová připojení podle názvů DNS můžete řídit pomocí pravidel součásti Kontrola webu. Pokud v pravidlech brány firewall potřebujete zadat název DNS:

- Zajistěte zabezpečení podnikové sítě LAN.

- Zajistěte zabezpečení mezipaměti a autoritativních serverů DNS.

- Povolte ochranu záznamu DNS před změnami.

Při vytváření pravidel síťových paketů mějte na paměti, že mají vyšší prioritu než pravidla sítě pro aplikace.

Metody vytváření pravidel 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.

Jak pomocí nástroje Sledování sítě vytvořit pravidlo síťových paketů v rozhraní aplikace

1. V hlavním okně aplikace v části **Monitorování** klikněte na dlaždici **Sledování sítě**.
2. Přejděte na 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 položku **Vytvořit síťové pravidlo balíčku**.

   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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Brána firewall**.
3. Klikněte na tlačítko **Pravidla paketů**.

   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
4. V rozevíracím seznamu **Přidat** vyberte umístění pravidla v seznamu: na začátku seznamu, na konci seznamu, nebo vedle vybraného pravidla.

   Pozice pravidla v seznamu určuje prioritu pravidla. Pravidlo na začátku seznamu má nejvyšší prioritu.
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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.
4. V bloku **Nastavení brány firewall** klikněte na tlačítko **Nastavení**.
   Tím otevřete seznam pravidel síťových paketů a seznam pravidel sítě aplikací.
5. Přejděte na kartu **Pravidla síťových paketů**.
   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
6. V rozevíracím seznamu **Přidat** vyberte umístění pravidla v seznamu: na začátku seznamu, na konci seznamu, nebo vedle vybraného pravidla.
   Pozice pravidla v seznamu určuje prioritu pravidla. Pravidlo na začátku seznamu má nejvyšší prioritu.
7. Do pole **Název** ručně zadejte název síťové služby.
8. 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.
9. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.
10. Uložte nové síťové pravidlo.
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. 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 **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Vyberte možnosti **Communication & Web Protection** → **Firewall**.
5. Vyberte kartu **Network packet rules**.
   Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
6. Klikněte na tlačítko **Add**.
   Otevře se formulář pro nové pravidlo sítě.
7. Do pole **Rule name** ručně zadejte název síťové služby.
8. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).
   Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Select rule template**. 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 **Log events**.
10. Uložte síťové pravidlo.

    Nové pravidlo sítě bude přidáno do seznamu.
11. Pomocí tlačítka **Move** 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 **Status** 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 všechny příchozí a odchozí síťové pakety. **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.
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)	Omezení kontroly síťových paketů jejich dobou života (Time to Live, 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, zadat rozsah IP adres nebo vybrat podsíť (Důvěryhodné sítě, Místní sítě, Veřejné sítě). Místo IP adresy můžete také zadat název DNS počítače. Názvy DNS byste měli používat pouze pro počítače LAN nebo interní služby. Interakce s cloudovými službami (jako je Microsoft Azure) a dalšími internetovými prostředky by měla zajišťovat součást Kontrola webu. Pokud jste v pravidle síťových paketů přidali název DNS, pro který nebylo možné určit IP adresu, aplikace Kaspersky Endpoint Security zobrazí varování. V seznamu pravidel síťových paketů ve webové konzole se přidá sloupec s popisem chyby. V konzole pro správu (MMC) není popis chyby k dispozici. Taková pravidla paketů jsou barevně zvýrazněna.
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, vytvořit samostatný seznam IP adres nebo zadat rozsah IP adres. Aplikace ukládá místní adresy pouze v případě, že je zadán seznam vzdálených adres, tj. v části **Vzdálené adresy** byla vybrána hodnota **Adresy ze seznamu** a byla přidána alespoň jedna adresa. 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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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**. Pokud je vybrána tato možnost, brána firewall použije na síťové připojení pravidla sítě 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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**/**Dolů** nastavte prioritu pravidla sítě.
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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.

4. V bloku **Nastavení brány firewall** klikněte na tlačítko **Nastavení**.

   Tím otevřete seznam pravidel síťových paketů a seznam pravidel sítě aplikací.

5. Přejděte na kartu **Pravidla síťových paketů**.

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. Uložte soubor.

      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. Otevřete soubor.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali 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 **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Vyberte možnosti **Communication & Web Protection** → **Firewall**.

5. Postup exportu seznamu pravidel v bloku **Network packet rules**:

   a. Vyberte pravidla, která chcete exportovat.

   b. Klikněte na tlačítko  → **Export**.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru JSON ve výchozí složce pro stahování.

6. Postup importu seznamu pravidel v bloku **Network packet rules**:

   a. Klikněte na tlačítko  → **Import**.

      V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam pravidel.

   b. Otevřete soubor.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.

7. Uložte změny.

Definování pravidel síťových paketů v jazyce XML

Brána firewall umožňuje exportovat pravidla síťových paketů ve formátu XML. Pak můžete soubor upravit, například přidat velké množství pravidel stejného typu.

Soubor XML obsahuje dva hlavní uzly: `Rules` a `Resources`. V uzlu `Rules` jsou uvedena pravidla síťových paketů. Tento uzel obsahuje pravidla nakonfigurovaná ve výchozím nastavení (*předdefinovaná pravidla*) i pravidla přidaná uživatelem (*vlastní pravidla*).

Kódování pravidel síťových paketů

```
<key name="0000">
<tDWORD name="RuleId">100</tDWORD>
<tDWORD name="RuleState">1</tDWORD>
<tDWORD name="RuleTypeId">4</tDWORD>
<tQWORD name="AppIdEx">0</tQWORD>
<tDWORD name="ResIdEx">812</tDWORD>
<tDWORD name="ResIdEx2">0</tDWORD>
<tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Nastavení pravidla síťových paketů ve formátu XML

Parametr	Popis	Hodnota
`<key name="0000">`	Priorita pravidla. Čím nižší hodnota, tím vyšší priorita.	Celé číslo Hodnota priority se musí skládat ze 4 číslic. Uzly v souboru XML musí být uspořádány podle hodnoty priority, počínaje hodnotou `0000`.
`RuleId`	ID pravidla.	Předdefinovaná pravidla `100` – **Požadavky na server DNS přes protokol TCP**. `101` – **Požadavky na server DNS přes protokol UDP**. `102` – **Odesílání e-mailových zpráv**. `110` – **Jakákoli síťová aktivita** (Důvěryhodné sítě). `125` – **Jakákoli síťová aktivita** (Místní sítě). `130` – **Síťová aktivita vzdálené plochy**. `131` – **Připojení TCP přes místní porty**. `132` – **Připojení UDP přes místní porty**. `133` – **Příchozí datový proud TCP**. `134` – **Příchozí datový proud UDP**. `137` – **Příchozí reakce na zprávu ICMP Cíl nedostupný**. `138` – **Příchozí pakety odpovědi na odezvu ICMP**. `140` – **Příchozí odezvy na zprávu ICMP Čas překročen**. `142` – **Příchozí datový proud ICMP**. `266` – **Příchozí pakety požadavku na odezvu ICMPv6**.
`RuleState`	Stav pravidla.	`0` – předdefinované pravidlo je zakázáno `1` – předdefinované pravidlo je povoleno `2` – vlastní pravidlo je zakázáno `3` – vlastní pravidlo je povoleno
`RuleTypeId`	ID typu pravidla.	`4` – Pravidla síťových paketů.
`AppIdEx`	ID aplikace, ke které pravidlo síťového paketu patří.	Pokud pravidlo nepatří k žádné aplikaci, hodnota je `0`.
`ResIdEx`	Hlavní ID prostředku s nastavením pravidel. Pomocí tohoto identifikátoru můžete vyhledávat blok s nastavením pravidel v uzlu `Resources`.	Celé číslo
`ResIdEx2`	ID typu sítě.	`0` – **Jakákoliv adresa**. `50` – **Důvěryhodné sítě**. `51` – **Místní sítě**. `52` – **Veřejné sítě**.

		`<Network Identifier>` – **Adresy ze seznamu** (adresy jsou definovány ručně).
`AccessFlag`	Hodnota parametru **Akce**.	`0` – **Povolit**. `2` – **Podle pravidel aplikace**. `3` – **Blokovat**. `4` – **Povolit** a **Protokolovat události**. `6` – **Podle pravidel aplikace** a **Protokolovat události**. `7` – **Blokovat** a **Protokolovat události**.

`</key>`

Uzel `Resources` obsahuje nastavení pravidel síťových paketů. Nastavení vlastních pravidel síťových paketů je uvedeno v bloku `<key name="0004">`.

Kódování vlastních pravidel síťových paketů

```
<key name="0026">
<key name="Data">
<key name="RemotePorts"> </key>
<key name="LocalPorts"> </key>
<key name="AdapterBindings">
<key name="0000">
<key name="IpAddresses">
<key name="0000">
<key name="IP">
<key name="V6">
<tQWORD name="Hi">0</tQWORD>
<tQWORD name="Lo">0</tQWORD>
<tDWORD name="Zone">0</tDWORD>
<tSTRING name="ZoneStr"/>
</key>
<tBYTE name="Version">4</tBYTE>
<tDWORD name="V4">16909060</tDWORD>
<tBYTE name="Mask">32</tBYTE>
</key>
<key name="AddressIP"> </key>
<tSTRING name="Address"/>
</key>
</key>
<key name="MacAddresses">
<key name="0000">
<tDWORD name="Type">0</tDWORD>
<tQWORD name="AddressData0">1108152157446</tQWORD>
<tQWORD name="AddressData1">0</tQWORD>
</key>
</key>
<tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
<tDWORD name="InterfaceType">3</tDWORD>
</key>
</key>
```

<tTYPE_ID name="unique">3213697024</tTYPE_ID>

<tBYTE name="Proto">2</tBYTE>

<tBYTE name="Direction">2</tBYTE>

<tBYTE name="IcmpType">0</tBYTE>

<tBYTE name="IcmpCode">0</tBYTE>

<tDWORD name="Flags">1</tDWORD>

<tBYTE name="TTL">255</tBYTE>

</key>

<key name="Childs"> </key>

<tDWORD name="Id">1073747214</tDWORD>

<tDWORD name="ParentID">7</tDWORD>

<tDWORD name="Flags">38</tDWORD>

<tSTRING name="Name">TEST1</tSTRING>

</key>

Nastavení vlastních pravidel síťových paketů

Parametr	Popis	Hodnota
`<key name="Data">`	ID bloku parametrů.	Celé číslo
`RemotePorts`	Hodnota parametru **Vzdálené porty**.	Seznam rozsahů vzdálených portů.
`LocalPorts`	Hodnota parametru **Místní porty**.	Seznam rozsahů místních portů.
`AdapterBindings`	Hodnota parametru **Síťové adaptéry**.	`IpAddresses` – hodnota parametru **IP adresy**. `MacAddresses` – hodnota parametru **Adresy MAC**. `AdapterName` – název síťového adaptéru. `InterfaceType` – hodnota parametru **Typ rozhraní**: • `0` – **Ostatní**. • `1` – **Zpětná smyčka**. • `2` – **Kabelová síť (Ethernet)**. • `3` – **Bezdrátová síť (Wi-Fi)**. • `4` – **Tunelové propojení**. • `5` – **PPP připojení**. • `6` – **PPPoE připojení**. • `7` – **VPN připojení**. • `8` – **Modemové připojení**.
`unique`	Interní ID struktury.	Celé číslo Doporučujeme ponechat tento parametr beze změny.
`Proto`	Hodnota parametru **Protokol**.	`0` – zakázáno. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.

`Direction`	Hodnota parametru **Směr**.	`1` – **Příchozí (paket)**. `2` – **Odchozí (paket)**. `3` – **Příchozí/odchozí**. `4` – **Příchozí**. `5` – **Odchozí**.
`IcmpType`	Hodnota parametru **Typ ICMP**.	Protokol ICMP `0` – **Odpověď odezvy** (ICMP) nebo zakázáno. `3` – **Cíl nedostupný** (ICMP). `4` – **Zdroj vyčerpán**. `5` – **Přesměrovat**. `6` – **Alternativní adresa hostitele**. `8` – **Požadavek odezvy**. `9` – **Inzerování směrovače**. `10` – **Oslovení směrovače**. `11` – **Čas překročen**. `12` – **Chybný parametr**. `13` – **Časová značka**. `14` – **Odpověď časové značky**. `15` – **Požadavek na informace**. `16` – **Odpověď s informacemi**. `17` – **Požadavek masky adresy**. `18` – **Odpověď masky adresy**. `30` – **Traceroute**. `31` – **Chyba převodu datagramu**. `32` – **Přesměrování mobilního hostitele**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Požadavek mobilní registrace**. `36` – **Odpověď mobilní registrace**. `37` – **Žádost o název domény**. `38` – **Odpověď na název domény**. `40` – **Photuris**. Protokol ICMPv6 `1` – **Cíl nedostupný**. `2` – **Paket je příliš velký**. `3` – **Čas překročen**. `4` – **Chybný parametr**. `128` – **Požadavek odezvy**. `129` – **Odpověď odezvy**. `130` – **Dotaz posluchače vícesměrového vysílání**. `131` – **Zpráva posluchače vícesměrového vysílání**. `132` – **Posluchač vícesměrového vysílání dokončen**. `133` – **Oslovení směrovače**. `134` – **Inzerování směrovače**. `135` – **Oslovení souseda**.

		`136` – **Inzerování souseda**. `137` – **Zpráva o přesměrování**. `138` – **Přečíslování směrovače**. `139` – **Dotaz na informace o uzlu ICMP**. `141` – **Zpráva oslovení inverzního protokolu Neighbor Discovery**. `142` – **Zpráva inzerování inverzního protokolu Neighbor Discovery**. `143` – **Verze 2 zprávy posluchače vícesměrového vysílání**. `144` – **Zpráva požadavku adresáře adresy domácího agenta**. `145` – **Zpráva odpovědi adresáře adresy domácího agenta**. `146` – **Oslovení mobilní předpony**. `147` – **Inzerování mobilní předpony**. `148` – **Zpráva oslovení cesty k certifikátu**. `149` – **Zpráva inzerování cesty k certifikátu**. `151` – **Inzerování směrovače vícesměrového vysílání**. `152` – **Oslovení směrovače vícesměrového vysílání**. `153` – **Ukončení směrovače vícesměrového vysílání**.
`IcmpCode`	Hodnota parametru **Kód ICMP**.	`0` – **Kód 0** nebo zakázáno. `1` – **Kód 1**. `2` – **Kód 2**.
`Flags`	Ukazatel atributu struktury.	Celé číslo Doporučujeme ponechat tento parametr beze změny.
`TTL`	Hodnota parametru **Doba života (TTL)**.	Hodnota v sekundách. Je-li tato možnost zakázána, hodnota je `0`.
`</key>`		
`Id`	Hlavní ID prostředku (viz uzel `Rules`).	Celé číslo
`ParentID`	ID nadřazené skupiny.	Celé číslo Doporučujeme ponechat tento parametr beze změny.
`Flags`	Stav pravidla.	`6` – pravidlo je zakázáno. `38` – pravidlo je povoleno.
`Name`	Název pravidla síťových paketů.	Řetězec

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 v části **Monitorování** klikněte na dlaždici **Sledování sítě**.
2. Přejděte na 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 sítě aplikace**.

   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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami** → **Brána firewall**.

3. Klikněte na tlačítko **Pravidla pro 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte možnosti **Základní ochrana před hrozbami** → **Brána firewall**.

4. V bloku **Nastavení brány firewall** klikněte na tlačítko **Nastavení**.

   Tím otevřete seznam pravidel síťových paketů a seznam pravidel sítě aplikací.

5. Přejděte na kartu **Síťová pravidla aplikace**.

6. Klikněte na tlačítko **Přidat**.

7. 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 ?.

8. 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.

9. Vyberte požadovanou aplikaci.

10. V rozevíracím seznamu **Přidat vybrané aplikace do skupiny důvěryhodnosti** vyberte položku **Výchozí skupiny** a klikněte na tlačítko **OK**.

    Aplikace bude přidána do výchozí skupiny.

11. Vyberte příslušnou aplikaci a poté vyberte možnost **Oprávnění aplikací** v místní nabídce aplikace.

    Otevře se okno pravidel a vlastností aplikace.

12. Vyberte kartu **Pravidla sítě**.

    Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.

13. Klikněte na tlačítko **Přidat**.

    Tím otevřete vlastnosti pravidla sítě.

14. Do pole **Název** ručně zadejte název síťové služby.

15. 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.

16. Chcete-li, aby byly akce pravidla sítě zahrnuty ve zprávě, zaškrtněte políčko **Protokolovat události**.

17. Uložte nové síťové pravidlo.

18. Pomocí tlačítek **Nahoru**/**Dolů** nastavte prioritu pravidla sítě.

19. Uložte změny.

Jak vytvořit pravidlo sítě aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Vyberte možnosti **Communication & Web Protection** → **Firewall**.

5. V bloku **Application rights and protected resources** klikněte na odkaz **Application rights**.

   Otevře se okno konfigurace oprávnění aplikace a seznam chráněných prostředků.

6. Přejděte na kartu **Application rights**.

   Na levé straně okna uvidíte seznam skupin důvěryhodnosti a na pravé straně jejich vlastnosti.

7. V bloku **Applications** klikněte na tlačítko **Add**.

   Spustí se průvodce přidáním aplikace do skupiny důvěryhodnosti.

8. Vyberte příslušnou skupinu důvěryhodnosti pro aplikaci.

9. Vyberte typ **Application**. Přejděte k dalšímu kroku.

   Pokud chcete vytvořit pravidlo sítě pro více aplikací, vyberte typ **Group** 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. Ukončete průvodce.

    Aplikace bude přidána do skupiny důvěryhodnosti.

12. V levé části okna vyberte příslušnou aplikaci.
13. V pravé části okna vyberte z rozevíracího seznamu možnost **Network rules**.

    Tím otevřete seznam výchozích pravidel sítě, která jsou nastavena bránou firewall.
14. Klikněte na tlačítko **Add**.

    Tím otevřete vlastnosti pravidla aplikace.
15. Do pole **Rule name** ručně zadejte název síťové služby.
16. Nakonfigurujte nastavení pravidla sítě (viz tabulka níže).

    Předdefinovanou šablonu pravidla můžete vybrat kliknutím na odkaz **Select rule template**. 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 **Log events**.
18. Uložte síťové pravidlo.

    Nové pravidlo sítě bude přidáno do seznamu.
19. Pomocí tlačítka **Move** 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, zadat rozsah IP adres nebo vybrat podsíť (Důvěryhodné sítě, Místní sítě, Veřejné sítě). Místo IP adresy můžete také zadat název DNS počítače. Názvy DNS byste měli používat pouze pro počítače LAN nebo interní služby. Interakce s cloudovými službami (jako je Microsoft Azure) a dalšími internetovými prostředky by měla zajišťovat součást Kontrola webu. Pokud jste v pravidle síťových paketů přidali název DNS, pro který nebylo možné určit IP adresu, aplikace Kaspersky Endpoint Security zobrazí varování. V seznamu pravidel síťových paketů ve webové konzole se přidá sloupec s popisem chyby. V konzole pro správu (MMC) není popis chyby k dispozici. Taková pravidla paketů jsou barevně zvýrazněna.
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, vytvořit samostatný seznam IP adres nebo zadat rozsah IP adres. Aplikace ukládá místní adresy pouze v případě, že je zadán seznam vzdálených adres, tj. v části **Vzdálené adresy** byla vybrána hodnota **Adresy ze seznamu** a byla přidána alespoň jedna adresa. 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.
3. Klikněte na tlačítko **Pravidla pro 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 u pravidla 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.
3. Klikněte na tlačítko **Pravidla pro 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.
3. Klikněte na tlačítko **Pravidla pro 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**.
   - **Zamítnout**.
   - **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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Základní ochrana před hrozbami → Brána firewall**.
3. Klikněte na tlačítko **Pravidla pro 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**/**Dolů** nastavte prioritu pravidla sítě.
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 v části **Monitorování** klikněte na dlaždici **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.

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.

Součást Prevence zneužití navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

Povolení a zakázání součásti Prevence zneužití

Ve výchozím nastavení je součást Prevence zneužití povolena a funguje v optimálním režimu. Kaspersky Endpoint Security sleduje spustitelné 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).

Jak povolit nebo zakázat součásti Prevence zneužití v konzole pro správu (MMC)

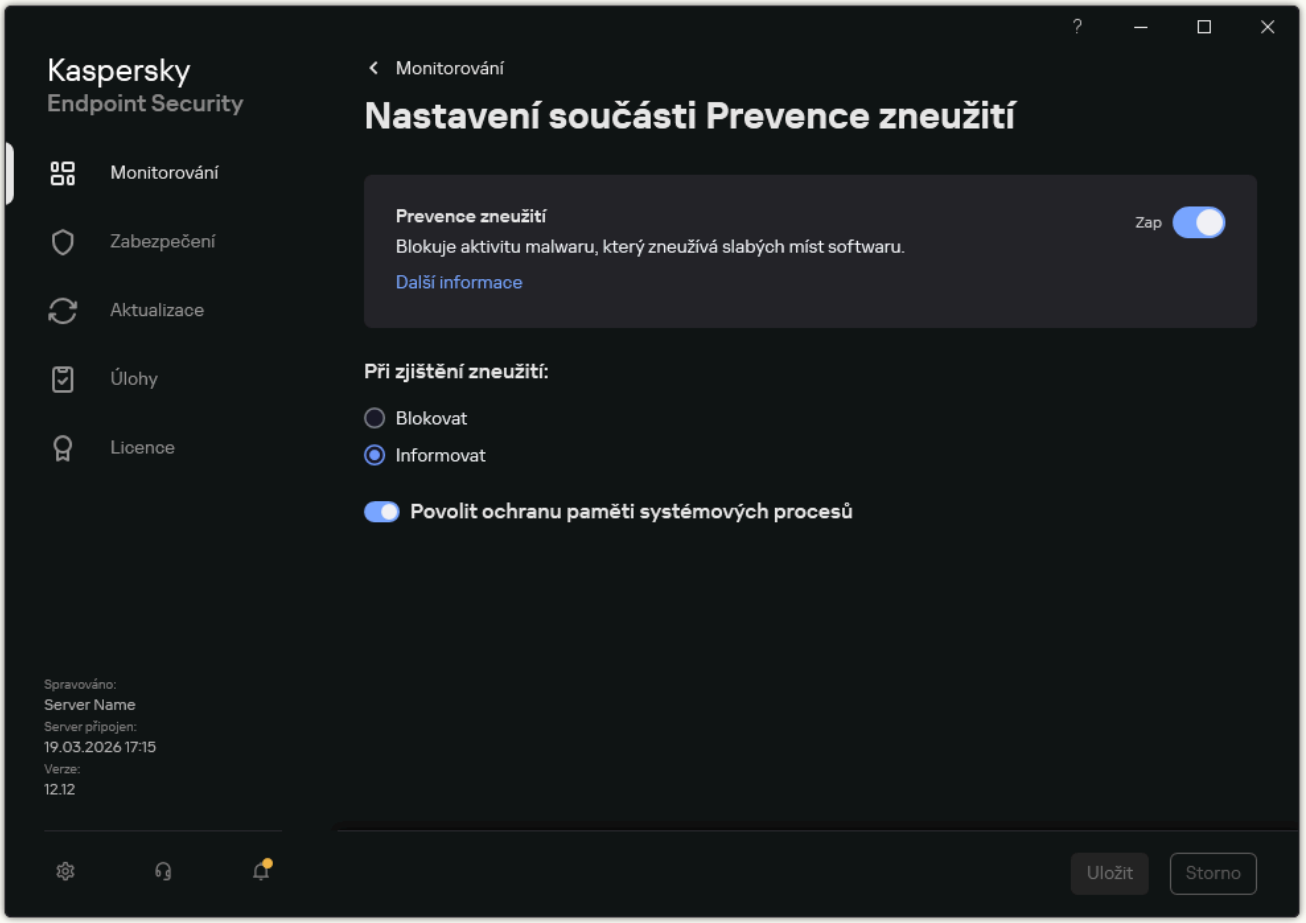
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence zneužití**.
4. Pomocí zaškrtávacího políčka **Prevence zneužití** můžete tuto součást povolit nebo zakázat.
5. V části **Při zjištění zneužití** vyberte příslušnou akci:
   - **Blokovat**. 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.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Prevence zneužití ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection → Behavior Analysis → Exploit Prevention**.
5. Pomocí přepínače **Exploit Prevention ENABLED** můžete tuto součást povolit nebo zakázat.
6. V části **Action on threat detection** vyberte příslušnou akci:
   - **Block**. 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.
   - **Inform or prompt for action**. 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.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Prevence zneužití v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Prevence zneužití**.



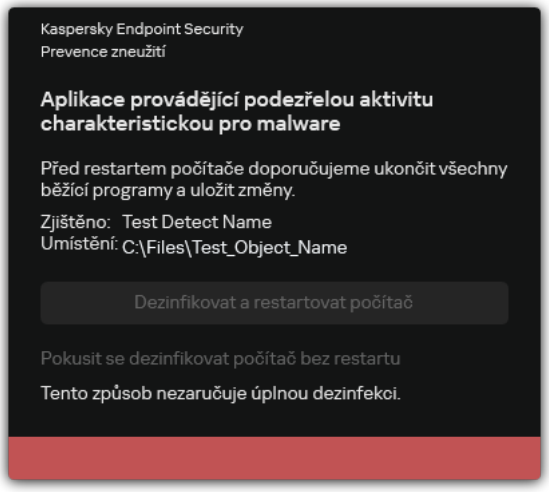
Nastavení součásti Prevence zneužití

3. Pomocí přepínače **Prevence zneužití** můžete tuto součást povolit nebo zakázat.

4. V části **Při zjištění zneužití** vyberte příslušnou akci:

   - **Blokovat**. 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.

5. Uložte změny.



Upozornění na aktivní hrozbu

Ochrana paměti systémových procesů

Ve výchozím nastavení je ochrana paměti systémových procesů povolená. Kaspersky Endpoint Security blokuje externí procesy, které se pokoušejí získat přístup k systémovým procesům.

Jak povolit nebo zakázat ochranu paměti systémových procesů v konzole pro správu (MMC)

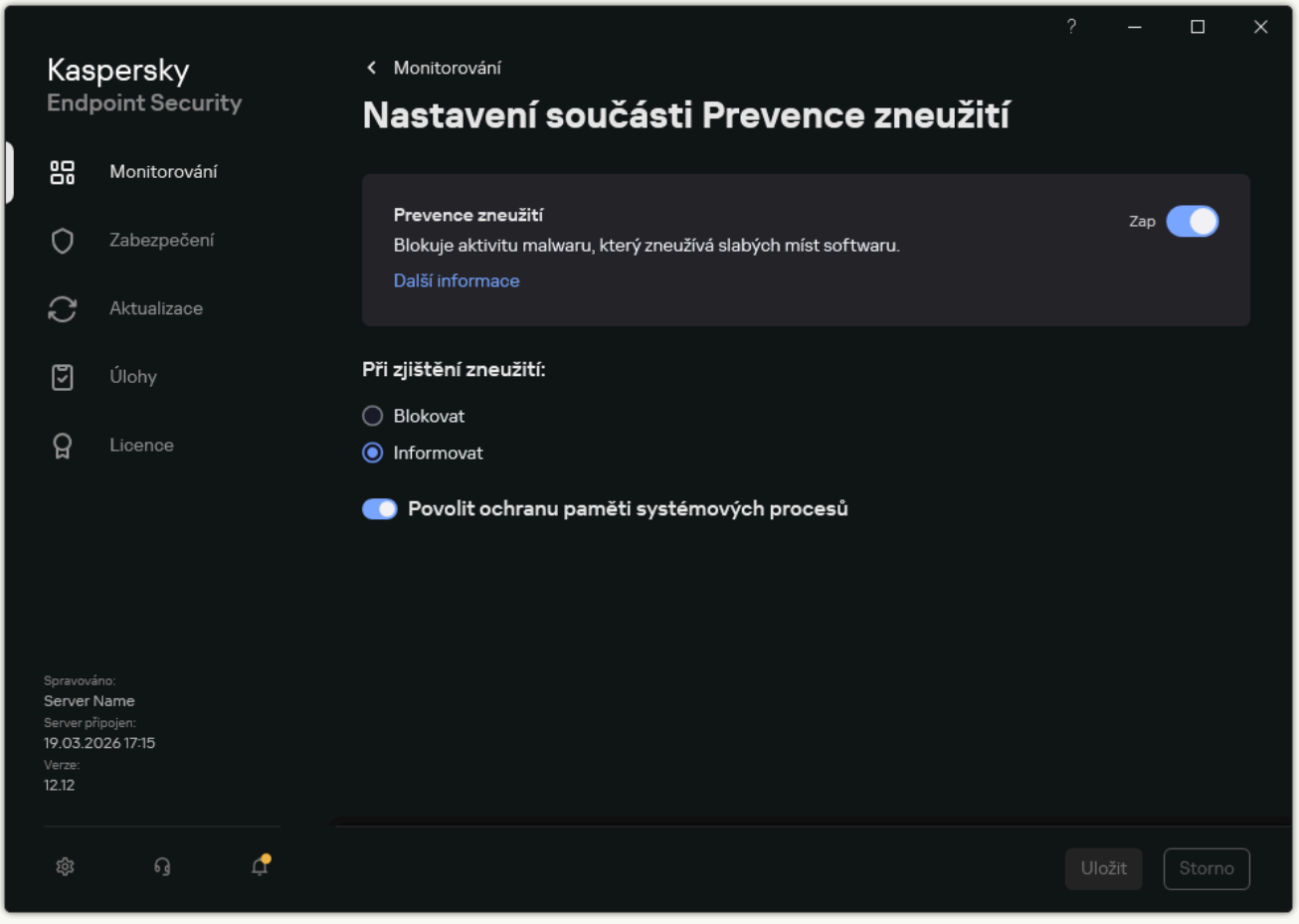
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Prevence zneužití**.
4. Pomocí zaškrtávacího políčka **Povolit ochranu paměti systémových procesů** můžete tuto možnost povolit nebo zakázat.
5. Uložte změny.

Jak povolit nebo zakázat ochranu paměti systémových procesů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection → Behavior Analysis → Exploit Prevention**.
5. Chcete-li povolit nebo zakázat tuto funkci, použijte přepínač **System process memory protection ENABLED**.
6. Uložte změny.

Jak povolit nebo zakázat ochranu paměti systémových procesů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Prevence zneužití**.



3. Chcete-li povolit nebo zakázat tuto funkci, použijte přepínač **Povolit ochranu paměti systémových procesů**.

4. Uložte změny.

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 je založeno na podpisech BSS a poskytuje aktivní ochranu počítače.

Součást Detekce chování navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

Ve výchozím nastavení je součást Detekce chování povolena a pracuje v režimu doporučeném odborníky společnosti Kaspersky. Když je zjištěna škodlivá aktivita, aplikace Kaspersky Endpoint Security odstraní spustitelný soubor příslušné škodlivé aplikace.

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.

Jak povolit nebo zakázat součást Detekce chování v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.

2. Ve stromu konzoly vyberte možnost **Policies**.

3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

4. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Detekce chování**.

5. Pomocí zaškrtávacího políčka **Detekce chování** můžete tuto součást povolit nebo zakázat.

6. V části **Akce při detekci aktivity malwaru** vyberte příslušnou akci:

   - **Odstranit**. 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.
   - **Blokovat**. 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.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Detekce chování ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection → Behavior Analysis → Behavior Detection**.

5. Pomocí přepínače **Behavior Detection ENABLED** můžete tuto součást povolit nebo zakázat.

6. V části **Action on threat detection** vyberte příslušnou akci:

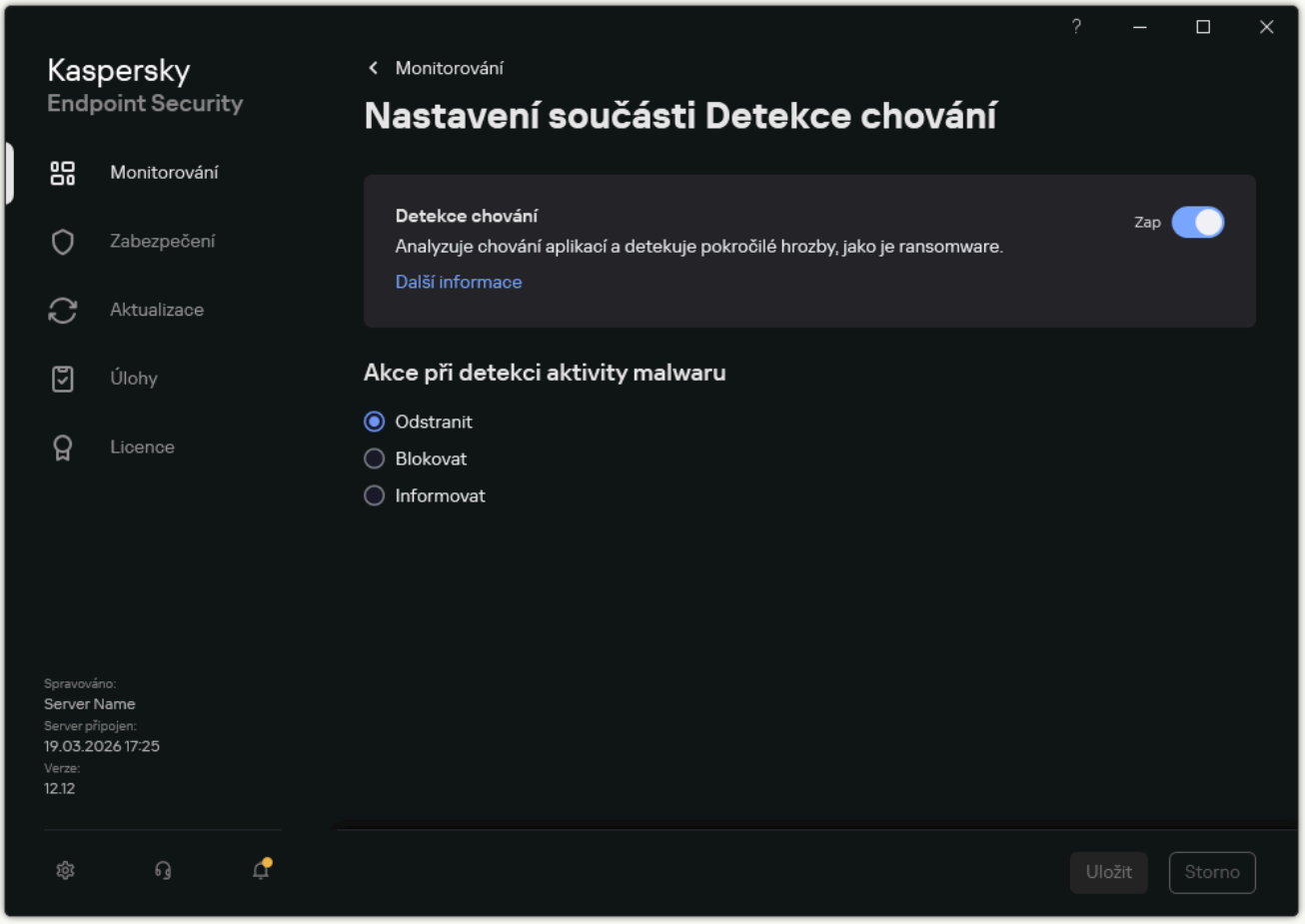
   - **Delete**. V případě, že je vybrána tato položka, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity odstraní spustitelný soubor škodlivého programu a vytvoří ve složce záloh jeho záložní kopii.
   - **Block**. Je-li tato položka vybrána, aplikace Kaspersky Endpoint Security při zjištění škodlivé aktivity ukončí tuto aplikaci.

- **Inform**. 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.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat součást Detekce chování v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Detekce chování**.



Nastavení součásti Detekce chování

3. Pomocí přepínače **Detekce chování** můžete tuto součást povolit nebo zakázat.
4. V části **Akce při detekci aktivity malwaru** vyberte příslušnou akci:
   - **Odstranit**. 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.
   - **Blokovat**. 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.
5. Uložte změny.

Pokud je součást Detekce chování povolena, aplikace Kaspersky Endpoint Security bude pomocí podpisů BSS analyzovat aktivitu aplikací v operačním systému.

Anti-Cryptor

Počínaje aplikací Kaspersky Endpoint Security 12.12 je ochrana sdílených složek před externím šifrováním, která bývala součástí součásti Detekce chování, samostatnou součástí, Anti-Cryptor.

Součást sleduje operace provedené pouze se soubory, které jsou uloženy na velkokapacitních paměťových zařízeních se souborovým systémem NTFS a které nejsou šifrovány systémem EFS.

Součást Anti-Cryptor 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.

Aby součást Anti-Cryptor fungovala, musíte povolit součást Detekce chování.

Pokud aplikace Kaspersky Endpoint Security zjistí pokus o úpravu souborů ve sdílených složkách, provede následující akce:

- Zablokuje přístup k úpravě souboru pro relaci, která iniciovala škodlivou aktivitu (soubor bude pouze pro čtení).
- Vytvoří záložní kopie souborů, které jsou upravovány.
- Přidá položku do zpráv o místním rozhraní aplikace a odešle informace o zjištěné škodlivé aktivitě do Kaspersky Security Center.
- Pokud je povolena součást Modul pro nápravu, upravené soubory jsou obnoveny ze záložních kopií.

Povolení a zakázání ochrany sdílených složek proti externímu šifrování

Ve výchozím nastavení je ochrana sdílených složek před externím šifrováním povolena a funguje podle doporučení odborníků společnosti Kaspersky. Chcete-li nakonfigurovat tuto funkci, můžete vytvořit rozsah ochrany a v případě potřeby nakonfigurovat výjimky. Ve výchozím nastavení aplikace automaticky identifikuje sdílené složky a monitoruje aktivitu souborů ve všech složkách. Když je zjištěn pokus o externí šifrování souborů ve sdílených složkách, aplikace Kaspersky Endpoint Security zablokuje relaci vzdáleného uživatele na jednu hodinu (ve výchozím nastavení).

Po nainstalování aplikace Kaspersky Endpoint Security bude fungování ochrany sdílených složek proti externímu šifrování omezené, dokud nebude počítač restartován.

Jak povolit nebo zakázat ochranu sdílených složek proti externímu šifrování v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.
4. Zaškrtávacím políčkem **Anti-Cryptor** můžete povolit nebo zakázat detekci aktivity, která je typická pro externí šifrování.
5. Vyberte příslušnou akci, kterou aplikace provede, když je detekován pokus o úpravu souborů ve sdílených složkách:
   - **Blokovat relaci po dobu N minut**. Je-li tato možnost vybrána, když aplikace Kaspersky Endpoint Security detekuje pokus o úpravu souborů ve sdílených složkách, zablokuje přístup k úpravám souborů pro relaci, která škodlivou aktivitu iniciovala, a vytvoří záložní kopie upravených souborů.

     Pokud je povolena součást Modul pro nápravu a je zaškrtnuta možnost **Blokovat relaci po dobu N minut**, změněné soubory se obnoví ze záložních kopií.

   - **Informovat**. Pokud je vybrána tato možnost, při zjištění pokusu o úpravu souborů ve sdílených složkách aplikace Kaspersky Endpoint Security přidá informace o tomto pokusu o úpravu seznamu aktivních hrozeb, přidá položku do zprávy o místním rozhraní aplikace a odešle informace o zjištěné škodlivé aktivitě do aplikace Kaspersky Security Center.
6. V případě potřeby upravte rozsah ochrany a definujte výjimky.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat ochranu sdílených složek proti externímu šifrování ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.

5. Pomocí přepínače **Anti-Cryptor ENABLED** můžete povolit nebo zakázat detekci aktivity, která je typická pro externí šifrování.

6. Vyberte příslušnou akci, kterou aplikace provede, když je detekován pokus o úpravu souborů ve sdílených složkách:

   - **Block connection for (min) N minut**. Je-li tato možnost vybrána, když aplikace Kaspersky Endpoint Security detekuje pokus o úpravu souborů ve sdílených složkách, zablokuje přístup k úpravám souborů pro relaci, která škodlivou aktivitu iniciovala, a vytvoří záložní kopie upravených souborů.

     Pokud je povolena součást Modul pro nápravu a je zaškrtnuta možnost **Block connection for (min) N minut**, změněné soubory se obnoví ze záložních kopií.

   - **Inform**. Pokud je vybrána tato možnost, při zjištění pokusu o úpravu souborů ve sdílených složkách aplikace Kaspersky Endpoint Security přidá informace o tomto pokusu o úpravu seznamu aktivních hrozeb, přidá položku do zprávy o místním rozhraní aplikace a odešle informace o zjištěné škodlivé aktivitě do aplikace Kaspersky Security Center.

7. V případě potřeby upravte rozsah ochrany a definujte výjimky.

8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat ochranu sdílených složek proti externímu šifrování v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.

3. Zaškrtávacím políčkem **Ochrana sdílených složek proti externímu šifrování** můžete povolit nebo zakázat detekci aktivity, která je typická pro externí šifrování.

4. Zaškrtávacím políčkem **Ochrana sdílených složek proti externímu šifrování** můžete povolit nebo zakázat detekci aktivity, která je typická pro externí šifrování.

5. Vyberte příslušnou akci, kterou aplikace provede, když je detekován pokus o úpravu souborů ve sdílených složkách:

   - **Blokovat připojení po dobu (min.) N minut**. Je-li tato možnost vybrána, když aplikace Kaspersky Endpoint Security detekuje pokus o úpravu souborů ve sdílených složkách, zablokuje přístup k úpravám souborů pro relaci, která škodlivou aktivitu iniciovala, a vytvoří záložní kopie upravených souborů.

     Pokud je povolena součást Modul pro nápravu a je zaškrtnuta možnost **Blokovat připojení po dobu (min.) N minut**, změněné soubory se obnoví ze záložních kopií.

   - **Informovat**. Pokud je vybrána tato možnost, při zjištění pokusu o úpravu souborů ve sdílených složkách aplikace Kaspersky Endpoint Security přidá informace o tomto pokusu o úpravu seznamu aktivních hrozeb, přidá položku do zprávy o místním rozhraní aplikace a odešle informace o zjištěné škodlivé aktivitě do aplikace Kaspersky Security Center.

6. V případě potřeby upravte rozsah ochrany a definujte výjimky.

7. Uložte změny.

Konfigurace doby blokování nedůvěryhodného počítače

Nedůvěryhodný počítač je vzdálený počítač, který se podílí na škodlivé aktivitě nebo šifrování dat. Ve výchozím nastavení Kaspersky Endpoint Security blokuje relaci vzdáleného uživatele na jednu hodinu. Po uplynutí doby blokování aplikace Kaspersky Endpoint Security odebere počítač ze seznamu blokování a obnoví přístup ke sdílené složce.

Jak konfigurovat dobu blokování nedůvěryhodného počítače v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.

4. V bloku **Akce při zjištění hrozby** vyberte **Blokovat relaci po dobu N min**.
5. Nakonfigurujte dobu blokování nedůvěryhodného počítače, který se podílí na škodlivé aktivitě nebo šifrování dat.
6. Uložte změny.

Jak konfigurovat dobu blokování nedůvěryhodného počítače ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. V části **Action on threat detection** nakonfigurujte dobu blokování nedůvěryhodného počítače, který se podílí na škodlivé aktivitě nebo šifrování dat.
6. Uložte změny.

Jak konfigurovat dobu blokování nedůvěryhodného počítače v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.
3. V bloku **Akce při zjištění hrozby** vyberte položku **Blokovat připojení po dobu (min.)**.
4. Nakonfigurujte dobu blokování nedůvěryhodného počítače, který se podílí na škodlivé aktivitě nebo šifrování dat.
5. Uložte změny.

Vzdálený počítač se tak uzamkne. Chcete-li vzdálený počítač odemknout, můžete restartovat aplikaci Kaspersky Endpoint Security.

Úprava rozsahu ochrany

Rozsah ochrany je seznam cest ke sdíleným složkám, ve kterých aplikace Kaspersky Endpoint Security monitoruje aktivitu souborů. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Ve výchozím nastavení aplikace automaticky identifikuje sdílené složky a monitoruje aktivitu souborů ve všech složkách.

Vyloučení složky z rozsahu ochrany 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.

Můžete také vyloučit počítače, z nichž nemají být zpracovávány pokusy o externí šifrování.

Jak upravit rozsah ochrany v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.
4. V bloku **Rozsah ochrany** vyberte položku **Pouze zadané sdílené složky**.
5. V seznamu složek klikněte na tlačítko **Přidat**.
6. Otevře se okno; v tomto okně zadejte cestu ke sdílené složce, kterou chcete zahrnout do rozsahu ochrany (například `C:\Share`).

Chcete-li přidat do rozsahu ochrany sdílenou složku, použijte místní cestu.

7. Klikněte na tlačítko **OK**.
8. V případě potřeby definujte výjimky z rozsahu ochrany:
   a. V bloku **Výjimky z kontroly** klikněte na tlačítko **Podle masky**.
   b. V okně, které se otevře, klikněte na tlačítko **Přidat**.
   c. V okně, které se zobrazí, určete příponu souboru ve formátu `*.<file extension>` nebo cestu ke složce. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.
      Aplikace nepodporuje některé přípony souborů výjimek. Můžete tedy určit výjimku jako `*.docx` nebo `**\Folder\**`.

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

Jak upravit rozsah ochrany ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. V bloku **Protection scope** vyberte položku **Only specified shared folders**.
6. V seznamu složek klikněte na tlačítko **Add**.
7. Otevře se okno; v tomto okně zadejte cestu ke sdílené složce, kterou chcete zahrnout do rozsahu ochrany (například `C:\Share`).

   Chcete-li přidat do rozsahu ochrany sdílenou složku, použijte místní cestu.
8. Klikněte na tlačítko **OK**.
9. V případě potřeby definujte výjimky z rozsahu ochrany:
   a. V pravé části okna klikněte na odkaz **Scan exclusions**.
   b. V okně, které se otevře, klikněte na tlačítko **Add**.
   c. V okně, které se zobrazí, určete příponu souboru ve formátu `*.<file extension>` nebo cestu ke složce. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.
      Aplikace nepodporuje některé přípony souborů výjimek. Můžete tedy určit výjimku jako `*.docx` nebo `**\Folder\**`.

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

Jak upravit rozsah ochrany v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.
3. V bloku **Rozsah ochrany** vyberte položku **Pouze zadané sdílené složky**.

4. V seznamu složek klikněte na tlačítko **Přidat**.

5. Otevře se okno; v tomto okně zadejte cestu ke sdílené složce, kterou chcete zahrnout do rozsahu ochrany (například `C:\Share`).

   Chcete-li přidat do rozsahu ochrany sdílenou složku, použijte místní cestu.

6. Klikněte na tlačítko **OK**.

7. V případě potřeby definujte výjimky z rozsahu ochrany:

   a. V pravé části okna klikněte na odkaz **Výjimky podle masky**.

   b. V okně, které se otevře, klikněte na tlačítko **Přidat**.

   c. V okně, které se zobrazí, určete příponu souboru ve formátu `*.<file extension>` nebo cestu ke složce. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.

   Aplikace nepodporuje některé přípony souborů výjimek. Můžete tedy určit výjimku jako `*.docx` nebo `**\Folder\**`.

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

8. Uložte změny.

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Výjimky a typy zjištěných objektů**.

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 rovněž 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

   Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

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.

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte do části **Trusted Zone**.

5. V okně, které se otevře, klikněte na odkaz **Malware Scan exclusions**.

6. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Merge values when inheriting**. 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 důvěryhodných aplikací, zaškrtněte políčko **Allow use of local exclusions**. 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam výjimek z kontroly v uživatelském rozhraní aplikace.

8. Klikněte na tlačítko **Add** a vyberte akci:

   - **Category**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
   - **New exclusion**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
   - **Select exclusion from list**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.

9. Vyberte, jak chcete výjimku přidat: **Path to the file or folder**.

10. Zadejte cestu ke sdílené složce.

    Cestu můžete rovněž 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

    Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `C:\Users\*\Folder\`.

11. V bloku **Apply exclusion to** vyberte součást **Behavior Detection**.

12. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Comment**.

13. Vyberte pro výjimku stav **Add to exclusions**.

    Pomocí přepínače můžete výjimku kdykoli ukončit.

14. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.

4. V bloku **Výjimky z kontroly a důvěryhodné aplikace** → **Výjimky z kontroly** klikněte na tlačítko **Nastavení**.

   Otevře se okno obsahující seznam výjimek z kontroly.

5. 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.

6. Pokud chcete uživateli umožnit vytvoření místního seznamu důvěryhodných aplikací, 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam výjimek z kontroly v uživatelském rozhraní aplikace.

7. Klikněte na tlačítko **Přidat** a vyberte akci:

   - **Kategorie**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
   - **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
   - **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.

8. Klikněte na tlačítko **Přidat**.

9. V bloku **Vlastnosti** zaškrtněte políčko **Soubor nebo složka**.

10. Kliknutím na odkaz **Vyberte soubor nebo složku** v bloku **Popis výjimky z kontroly (kliknutím na podtržené položky je můžete upravit)** otevřete okno **Název souboru nebo složky**.

11. Klikněte na tlačítko **Procházet** a vyberte sdílenou složku.

    Cestu můžete rovněž 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

    Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

12. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

13. Kliknutím na odkaz v bloku **Popis výjimky z kontroly (kliknutím na podtržené položky je můžete upravit)** otevřete okno **Součásti ochrany**.

14. Zaškrtněte políčko vedle součásti **Detekce chování**.

15. Uložte změny.

Přidávání důvěryhodných počítačů pro externí šifrování dat

Pokud vaše organizace používá ve svém pracovním postupu výměny souborů externí šifrování dat, musíte vytvořit seznam důvěryhodných počítačů. Kaspersky Endpoint Security nesleduje šifrování dat na důvěryhodných počítačích.

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.

Změnu seznamu důvěryhodných počítačů mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak přidat důvěryhodný počítač pro šifrování externích dat v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Anti-Cryptor**.
4. V bloku **Výjimky z kontroly** klikněte na tlačítko **Podle názvu nebo IP adresy**.
5. V okně, které se otevře, klikněte na tlačítko **Podle názvu nebo IP adresy**.
6. Zadejte IP adresy, rozsah IP adres nebo názvy počítačů, ze kterých nesmí být zpracovávány pokusy o externí šifrování.
   Příklady:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
7. Uložte změny.

Jak přidat důvěryhodný počítač pro šifrování externích dat ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. V pravé části okna klikněte na odkaz **Exclusions by name or IP address**.
6. V okně, které se otevře, klikněte na tlačítko **Add**.
7. Zadejte IP adresy, rozsah IP adres nebo názvy počítačů, ze kterých nesmí být zpracovávány pokusy o externí šifrování.
   Příklady:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Uložte změny.

Jak přidat důvěryhodný počítač pro externí šifrování dat v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Anti-Cryptor**.
3. V pravé části okna klikněte na odkaz **Výjimky podle názvu nebo IP adresy**.
4. V okně, které se otevře, klikněte na tlačítko **Přidat**.
5. Zadejte IP adresy, rozsah IP adres nebo názvy počítačů, ze kterých nesmí být zpracovávány pokusy o externí šifrování.
   Příklady:
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
6. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Anti-Cryptor**.
4. V bloku **Výjimky z kontroly** klikněte na tlačítko **Podle názvu nebo IP adresy**.
5. 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 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. Uložte soubor.
   Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.
6. 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. Otevřete soubor.

Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

7. Uložte změny.

[Jak exportovat a importovat seznam výjimek ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Klikněte na odkaz **Exclusions by name or IP address**.
6. Postup exportu seznamu pravidel:
   a. Vyberte výjimky, které chcete exportovat.
   b. Klikněte na tlačítko → **Export**.
   Aplikace Kaspersky Endpoint Security exportuje seznam výjimek do souboru JSON ve výchozí složce pro stahování.
7. Postup importu seznamu výjimek:
   a. Klikněte na tlačítko → **Import**.
   V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam výjimek.
   b. Otevřete soubor.
   Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru JSON přidá nové položky.
8. Uložte změny.

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 kontroly malwaru.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami → Modul pro nápravu**.
4. Pomocí zaškrtávacího políčka **Modul pro nápravu** můžete tuto součást povolit nebo zakázat.
5. Uložte změny.

Jak povolit nebo zakázat součást Modul pro nápravu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Host Threat Protection → Behavior Analysis → Remediation Engine**.
5. Pomocí přepínače **Remediation Engine ENABLED** můžete tuto součást povolit nebo zakázat.
6. Uložte změny.

Jak povolit nebo zakázat součást Modul pro nápravu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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.

Kaspersky Security Network



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.

Funkce KSN nemusí být v softwaru dostupná na území USA.

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 reputaci kontrolovaných webových adres a také informace o reputaci kategorii a reputaci kontrolovaných souborů.

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 Kaspersky Security Network a na webových stránkách společnosti Kaspersky. Soubor ksn_<ID jazyka>.txt s textem prohlášení o Kaspersky Security Network je součástí distribučního balíčku aplikace.

Infrastruktura databází reputace společnosti Kaspersky

Kaspersky Endpoint Security podporuje následující infrastrukturní řešení pro práci s databázemi reputace Kaspersky:

- *Kaspersky Security Network (KSN)* je řešení, které používá většina aplikací Kaspersky. Účastníci služby KSN získávají od společnosti Kaspersky informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází reputace a statistik.
- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

Povolení a zakázání používání služby Kaspersky Security Network

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.

Jak povolit nebo zakázat používání KSN v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Kaspersky Security Network**.
4. Pomocí přepínače **Kaspersky Security Network** můžete tuto součást povolit nebo zakázat.

   Pokud jste povolili použití KSN, aplikace Kaspersky Endpoint Security zobrazí prohlášení o Kaspersky Security Network. Pokud s nimi souhlasíte, přečtěte si a přijměte podmínky používání uvedené v Prohlášení o Kaspersky Security Network (KSN).
5. V případě potřeby zrušte zaškrtnutí políčka **Povolit rozšířený režim KSN**.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat používání KSN ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Kaspersky Security Network**.
5. Pomocí přepínače **Use of Kaspersky Security Network (KSN) ENABLED** můžete tuto součást povolit nebo zakázat.

   Pokud jste povolili použití KSN, aplikace Kaspersky Endpoint Security zobrazí prohlášení o Kaspersky Security Network. Pokud s nimi souhlasíte, přečtěte si a přijměte podmínky používání uvedené v Prohlášení o Kaspersky Security Network (KSN).

6. V případě potřeby přepínač **Use extended KSN mode** vypněte.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat používání KSN v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Rozšířená ochrana před hrozbami → Kaspersky Security Network**.

3. Pomocí přepínače **Kaspersky Security Network** můžete tuto součást povolit nebo zakázat.

   Pokud jste povolili použití KSN, aplikace Kaspersky Endpoint Security zobrazí prohlášení o Kaspersky Security Network. Pokud s nimi souhlasíte, přečtěte si a přijměte podmínky používání uvedené v Prohlášení o Kaspersky Security Network (KSN).

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 služby Kaspersky Private Security Network

Kaspersky Private Security Network (KPSN) 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. Kaspersky Private Security Network (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 *Nedůvěryhodné*, ale v KSN/KPSN má reputaci *Důvěryhodné*, aplikace Kaspersky Endpoint Security soubor detekuje jako *Nedůvěryhodné* 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 vůči službě 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.

- Kaspersky Endpoint Security v režimu Light Agent komunikuje se servery KSN prostřednictvím proxy serveru KSN. Přímá komunikace s KSN není podporována.

Povolení a zakázání režimu cloudu pro součásti ochrany

Režim cloudu 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.

Pokud aplikace funguje v režimu Light Agent, režim cloudu není k dispozici.

Jak povolit nebo zakázat režim cloudu u součástí ochrany v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Kaspersky Security Network**.
4. Pomocí zaškrtávacího políčka **Povolit režim cloudu** můžete tuto součást povolit nebo zakázat.
5. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat režim cloudu u součástí ochrany ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Kaspersky Security Network**.
5. Pomocí přepínače **Use cloud mode** můžete tuto součást povolit nebo zakázat.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit nebo zakázat režim cloudu u součástí ochrany v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **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.

Nastavení proxy serveru KSN

Uživatelské počítače spravované administračním serverem Kaspersky Security Center mohou se sítí KSN komunikovat přímo nebo prostřednictvím služby KSN Proxy.

Pokud je aplikace spuštěna v režimu Light Agent, přímá komunikace s KSN není podporována. Kaspersky Endpoint Security komunikuje se servery KSN prostřednictvím proxy serveru KSN.

Služba KSN Proxy poskytuje následující možnosti:

- Počítač uživatele může odesílat dotazy a informace do služby KSN i bez přímého přístupu k internetu.
- Služba KSN Proxy ukládá zpracovaná data do mezipaměti, čímž snižuje zatížení komunikačního kanálu a externí sítí a urychluje příjem informací, které jsou uživatelským počítačem požadovány.

Ve výchozím nastavení platí, že po povolení sítě KSN a přijetí prohlášení o KSN používá aplikace k připojení k síti Kaspersky Security Network proxy server. Proxy server používaný aplikací je server pro správu aplikace Kaspersky Security Center prostřednictvím portu TCP 13111. Pokud proxy server KSN není k dispozici, musíte ověřit následující:

- Na serveru pro správu je spuštěna služba `ksnproxy`.

- Brána firewall v počítači neblokuje port 13111.

Použití služby KSN Proxy můžete nakonfigurovat takto: povolte nebo zakažte KSN Proxy a nakonfigurujte port pro připojení. K tomu musíte otevřít vlastnosti serveru pro správu. Další informace o konfiguraci služby KSN Proxy najdete v nápovědě k aplikaci Kaspersky Security Center. Službu KSN Proxy můžete také povolit nebo zakázat u jednotlivých počítačů v zásadě aplikace Kaspersky Endpoint Security.

Jak povolit nebo zakázat proxy server KSN v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Rozšířená ochrana před hrozbami** → **Kaspersky Security Network**.
4. V bloku **Nastavení proxy serveru KSN** povolte nebo zakažte proxy serveru KSN pomocí zaškrtávacího políčka **Použít jako proxy server KSN server pro správu**.
5. V případě potřeby zaškrtněte políčko **Použít servery KSN, pokud není proxy server KSN k dispozici**.

   Pokud je zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security použije servery KSN v případě nedostupnosti služby KSN Proxy. Servery KSN mohou být umístěny na straně společnosti Kaspersky a u třetí strany (při použití služby Kaspersky Private Security Network).
6. Uložte změny.

Jak povolit nebo zakázat proxy server KSN ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Kaspersky Security Network**.
5. Pomocí zaškrtávacího políčka **Use Administration Server as a KSN proxy server** můžete povolit nebo zakázat KSN Proxy.
6. V případě potřeby zaškrtněte políčko **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.

   Pokud je zaškrtnuto toto políčko, aplikace Kaspersky Endpoint Security použije servery KSN v případě nedostupnosti služby KSN Proxy. Servery KSN mohou být umístěny na straně společnosti Kaspersky a u třetí strany (při použití služby Kaspersky Private Security Network).
7. Uložte změny.

Adresa služby KSN Proxy odpovídá adrese serveru pro správu. Pokud dojde ke změně názvu domény serveru pro správu, musíte ručně aktualizovat adresu KSN Proxy.

Postup konfigurace adresy proxy serveru KSN:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole vyberte možnosti **Advanced** → **Remote installation** → složku **Installation packages**.
3. V místní nabídce složky **Installation packages** vyberte možnost **Properties**.
4. V okně, které se otevře, na kartě **General** zadejte novou adresu proxy serveru KSN.
5. Uložte změny.

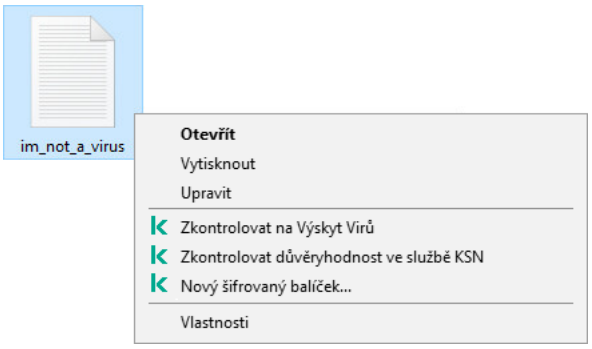
Kontrola důvěryhodnosti souboru ve službě Kaspersky Security Network

Pokud pochybujete o bezpečnosti souboru, můžete zkontrolovat jeho důvěryhodnost ve službě Kaspersky Security Network.

Pokud jste přijali podmínky prohlášení o Kaspersky Security Network, můžete zkontrolovat reputaci souboru.

Postup kontroly důvěryhodnosti souboru ve službě Kaspersky Security Network:

Otevřete místní nabídku souboru a vyberte možnost **Zkontrolovat důvěryhodnost ve službě KSN** (viz obrázek níže).



Místní nabídka Soubor

Aplikace Kaspersky Endpoint Security zobrazuje důvěryhodnost souboru:

Důvěryhodné (Kaspersky Security Network). Aplikace považuje soubor za důvěryhodný, pokud je splněna jedna nebo více z následujících podmínek:

- soubor je digitálně podepsán důvěryhodným dodavatelem;
- soubor má důvěryhodnou reputaci ve službě Kaspersky Security Network;
- uživatel zařadil soubor do skupiny Důvěryhodné.

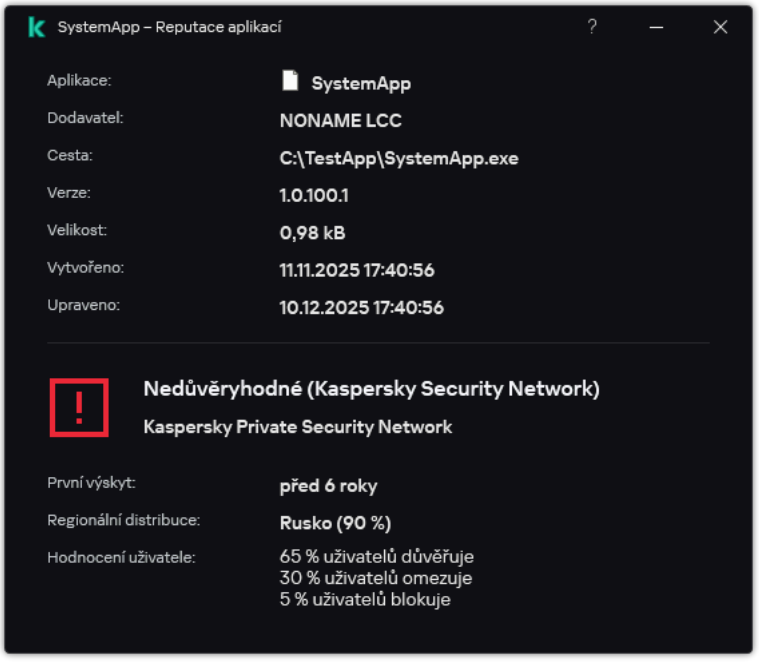
Legitimní software, který mohou použít útočníci k poškození počítače nebo osobních dat. I když tyto aplikace nemají žádnou škodlivou funkci, mohou být zneužity útočníky. Podrobnosti o legitimním softwaru, který může být využíván pachateli k poškození počítače nebo osobních údajů uživatele, najdete na webu encyklopedie IT Kaspersky. Tyto aplikace můžete přidat na seznam důvěryhodných zařízení.

Nedůvěryhodné (Kaspersky Security Network). Virus nebo jiná aplikace, které představují hrozbu.

Neznámá (Kaspersky Security Network). Kaspersky Security Network nemá o souboru žádné informace. oubor 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: *Kaspersky Security Network* nebo *Kaspersky Private Security Network*.

Aplikace Kaspersky Endpoint Security také zobrazuje další informace o souboru (viz obrázek níže).



Důvěryhodnost souboru ve službě Kaspersky Security Network

Kontrola šifrovaných připojení

Po instalaci přidá aplikace Kaspersky Endpoint Security certifikát Kaspersky do systémového úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Kaspersky Endpoint Security používá tento certifikát ke kontrole šifrovaného připojení. 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, Detekce chování a Prevence zneužití 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

Povolení kontroly šifrovaného připojení

Ve výchozím nastavení aplikace Kaspersky Endpoint Security nekontroluje šifrovaná připojení vždy, ale pouze na žádost součástí ochrany.

Jak povolit kontrolu šifrovaných připojení v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.
5. V bloku **Kontrola šifrovaných připojení** vyberte režim kontroly šifrovaného připojení:
   - **Kontrola šifrovaného 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 webovými 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.
6. V případě potřeby přidejte výjimky z kontroly: důvěryhodné adresy a aplikace.
7. Nakonfigurujte nastavení pro kontrolu šifrovaných připojení (viz tabulka níže).
8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit kontrolu šifrovaných připojení ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. V části **Encrypted Connections Scan** zapněte přepínač **Encrypted Connections Scan ENABLED**.
   Pokud je přepínač vypnutý, aplikace Kaspersky Endpoint Security nebude mít přístup k obsahu webů, jejichž adresa začíná na `https://`.
6. Klikněte na možnost **Settings** a vyberte režim kontroly šifrovaného připojení:
   - **Scan encrypted connections upon request from protection components**. Aplikace Kaspersky Endpoint Security bude kontrolovat šifrované přenosy, pouze pokud o to požádají součásti Ochrana před webovými hrozbami, Ochrana před hrozbami v poště nebo Kontrola

webu.

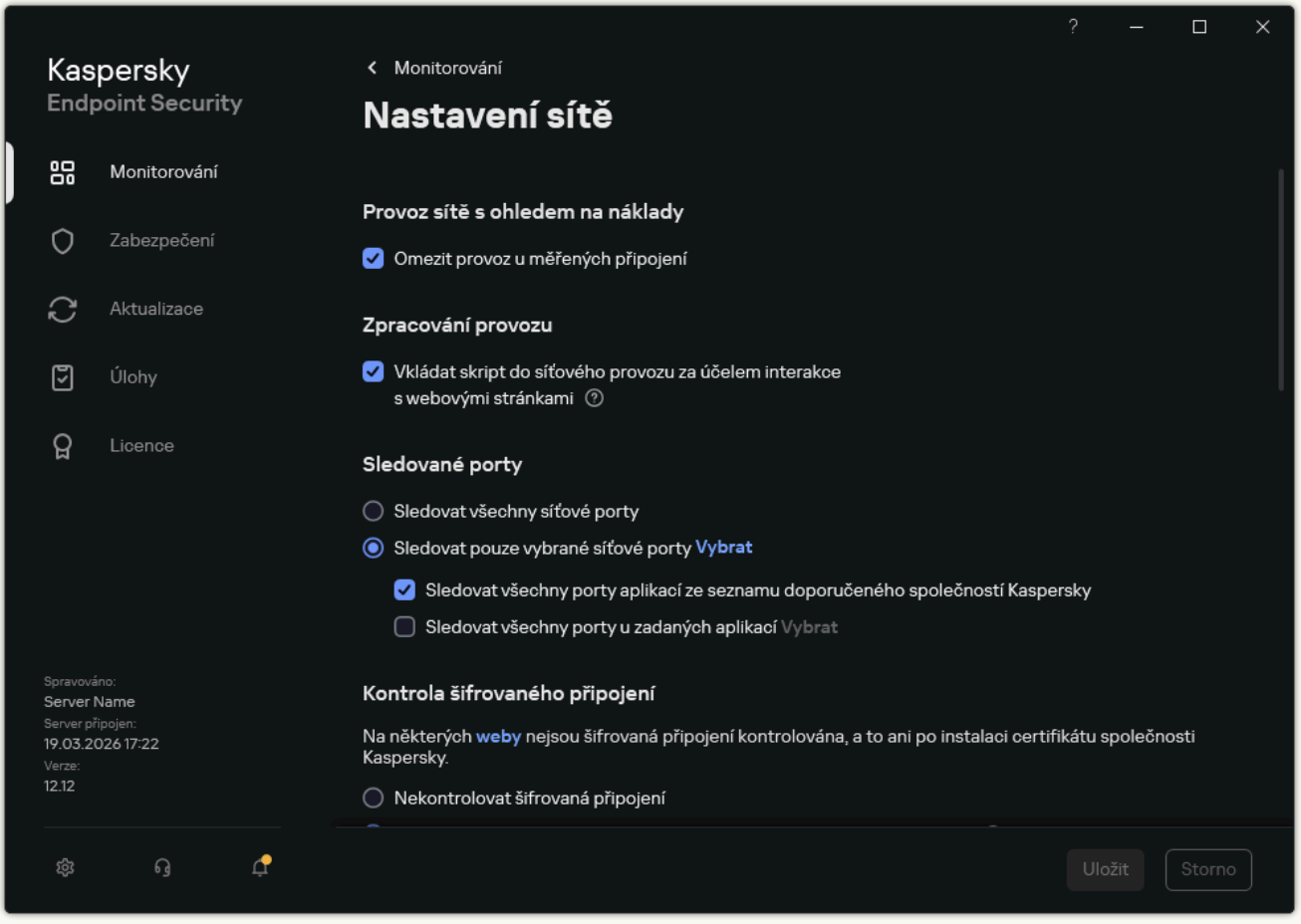
- **Always scan encrypted connections**. Aplikace Kaspersky Endpoint Security bude kontrolovat šifrovaný provoz, i když jsou zakázány součásti ochrany.

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.

7. V případě potřeby přidejte výjimky z kontroly: důvěryhodné adresy a aplikace.
8. Nakonfigurujte nastavení pro kontrolu šifrovaných připojení (viz tabulka níže).
9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit kontrolu šifrovaných připojení v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.



Nastavení kontroly šifrovaných připojení

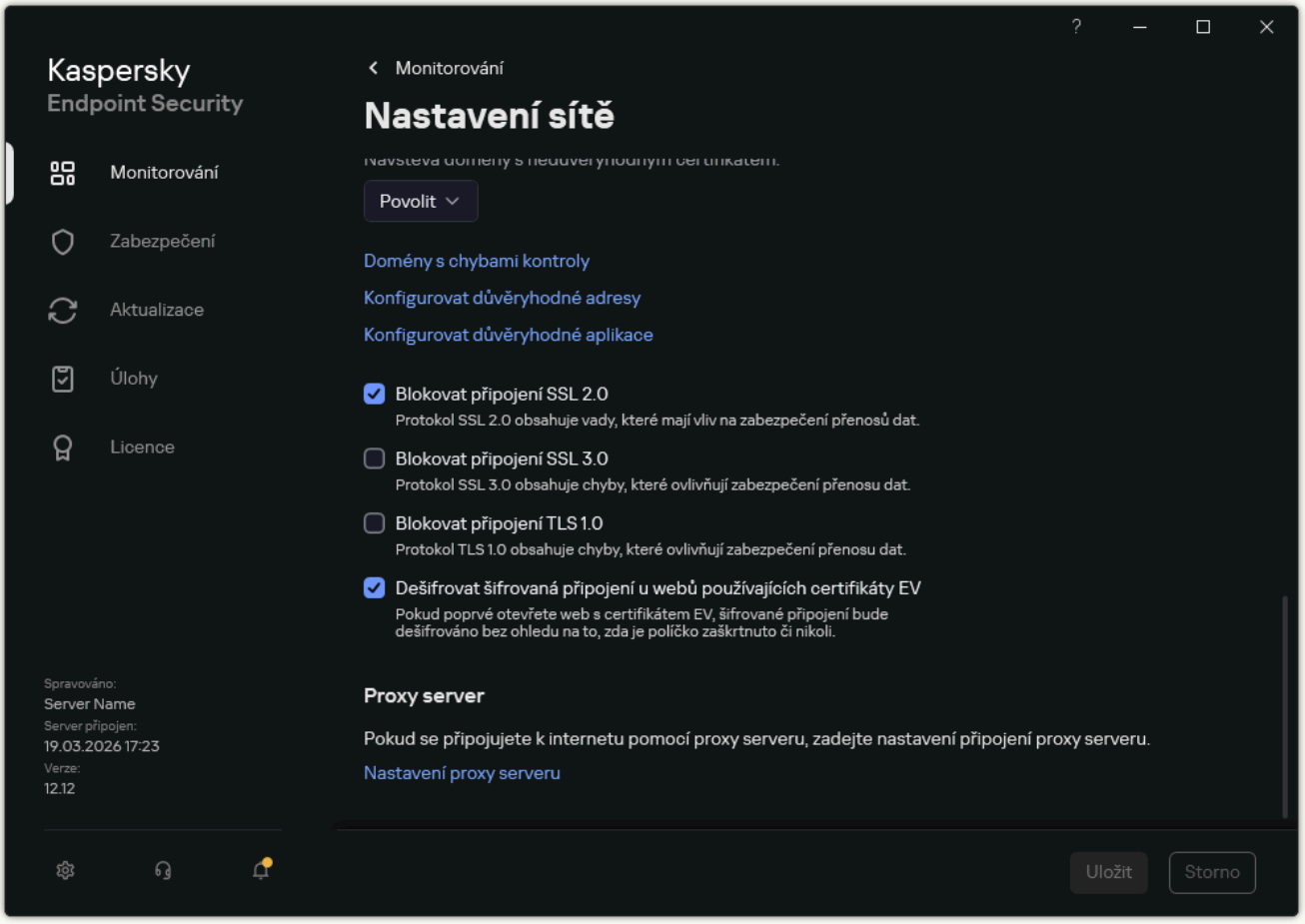
3. V bloku **Kontrola šifrovaného připojení** vyberte režim kontroly šifrovaného připojení:

- **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 webovými 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. Nakonfigurujte nastavení pro kontrolu šifrovaných připojení (viz tabulka níže).



Další nastavení pro kontrolu šifrovaných připojení

6. Uložte změny.

Nastavení kontroly šifrovaných připojení

Parametr	Popis
Důvěryhodné kořenové certifikáty	Seznam důvěryhodných kořenových certifikátů. Aplikace Kaspersky Endpoint Security umožňuje instalovat do uživatelských počítačů důvěryhodné kořenové certifikáty, pokud například potřebujete nasadit nové certifikační centrum. Aplikace umožňuje přidat certifikát do speciálního úložiště certifikátů Kaspersky Endpoint Security. V tomto případě je certifikát považován za důvěryhodný pouze pro aplikaci Kaspersky Endpoint Security. Jinými slovy, uživatel může získat přístup k webu s novým certifikátem v prohlížeči. Pokud se k webovému serveru pokusí získat přístup jiná aplikace, může dojít k chybě připojení z důvodu problému s certifikátem. K přidání do systémového úložiště certifikátů můžete použít zásady skupin služby Active Directory.

Návštěva domény s nedůvěryhodným certifikátem	• **Povolit**. 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. Pokud aplikace nebo služba třetí strany naváže spojení s doménou s nedůvěryhodným certifikátem, Kaspersky Endpoint Security vytvoří svůj vlastní certifikát pro kontrolu provozu. Nový certifikát má stav *Nedůvěryhodné*. To je nutné pro upozornění aplikace třetí strany na nedůvěryhodné připojení, protože v tomto případě nelze zobrazit stránku HTML a připojení lze navázat v režimu na pozadí. • **Blokovat**. Při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security zablokuje 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.
Návštěva domény s chybou kontroly šifrovaných připojení	• **Blokovat**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení blokuje síťové připojení. • **Povolit a přidat doménu k výjimkám**. 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**. Kaspersky Endpoint Security také vytvoří událost pro chybu kontroly šifrovaného připojení.
Blokovat připojení SSL 2.0	Pokud je políčko zaškrtnuto, aplikace monitoruje a blokuje síťová připojení vytvořená pomocí protokolu SSL 2.0. Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu SSL 2.0. Aplikace však nemonitoruje síťový provoz přes tento protokol.
Blokovat připojení SSL 3.0	Pokud je políčko zaškrtnuto, aplikace blokuje síťová připojení vytvořená pomocí protokolu SSL 3.0. Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu SSL 3.0. Aplikace monitoruje síťový provoz přes tento protokol. Všechny součásti aplikace fungují bez omezení.
Blokovat připojení TLS 1.0	Pokud je políčko zaškrtnuto, aplikace blokuje síťová připojení vytvořená pomocí protokolu TLS 1.0. Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu TLS 1.0. Aplikace monitoruje síťový provoz přes tento protokol. Všechny součásti aplikace fungují bez omezení.
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 dešifruje a monitoruje šifrovaná připojení a weby, které používají certifikát EV. Jestliže toto políčko není zaškrtnuté, aplikace nemá přístup k obsahu provozu HTTPS. Z tohoto důvodu aplikace monitoruje provoz HTTPS pouze na základě adresy webových stránek, například `https://bing.com`. Pokud poprvé otevíráte web s certifikátem EV, šifrované připojení bude dešifrováno bez ohledu na to, zda je toto políčko zaškrtnuto.

Instalace důvěryhodných kořenových certifikátů

Aplikace Kaspersky Endpoint Security umožňuje instalovat do uživatelských počítačů důvěryhodné kořenové certifikáty, pokud například potřebujete nasadit nové certifikační centrum. Aplikace umožňuje přidat certifikát do speciálního úložiště certifikátů Kaspersky Endpoint Security. V tomto případě je certifikát považován za důvěryhodný pouze pro aplikaci Kaspersky Endpoint Security. Jinými slovy, uživatel může získat přístup k webu s novým certifikátem v prohlížeči. Pokud se k webovému serveru pokusí získat přístup jiná aplikace, může dojít k chybě připojení z důvodu problému s certifikátem. K přidání do systémového úložiště certifikátů můžete použít zásady skupin služby Active Directory.

Změnu seznamu důvěryhodných kořenových certifikátů mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak instalovat důvěryhodné kořenové certifikáty v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.
4. V bloku **Důvěryhodné kořenové certifikáty** klikněte na tlačítko **Přidat**.
5. Tím otevřete okno; v tomto okně vyberte důvěryhodný kořenový certifikát.
   Kaspersky Endpoint Security podporuje certifikáty s příponami PEM, DER a CRT.
6. Uložte změny.

Jak instalovat důvěryhodné kořenové certifikáty ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. Klikněte na odkaz **Trusted root certificates**.
6. Tím otevřete okno; v tomto okně klikněte na tlačítko **Add** a vyberte důvěryhodný kořenový certifikát.
   Kaspersky Endpoint Security podporuje certifikáty s příponami PEM, DER a CRT.
7. Uložte změny.

Jak instalovat důvěryhodné kořenové certifikáty v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.
3. V bloku **Kontrola šifrovaného připojení** klikněte na tlačítko **Zobrazit certifikáty**.
4. Tím otevřete okno; v tomto okně klikněte na tlačítko **Přidat** a vyberte důvěryhodný kořenový certifikát.
   Kaspersky Endpoint Security podporuje certifikáty s příponami PEM, DER a CRT.
5. Uložte změny.

V důsledku toho používá aplikace Kaspersky Endpoint Security při kontrole provozu kromě systémového úložiště certifikátů také své vlastní úložiště certifikátů.

Kontrola šifrovaných připojení s nedůvěryhodným certifikátem

Po instalaci přidá aplikace Kaspersky Endpoint Security certifikát Kaspersky do systémového úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Kaspersky Endpoint Security používá tento certifikát ke kontrole šifrovaného připojení. Při návštěvě domény s nedůvěryhodným certifikátem můžete uživateli povolit nebo zakázat přístup k této doméně (viz pokyny níže).

Pokud jste uživateli povolili navštěvovat domény s nedůvěryhodnými certifikáty, Kaspersky Endpoint Security provede následující akce:

- Při návštěvě domény s nedůvěryhodným certifikátem v *prohlížeči* aplikaci Kaspersky Endpoint Security používá ke kontrole provozu certifikát Kaspersky. Kaspersky Endpoint Security zobrazí HTML stránku s upozorněním a informací o důvodu, proč není doporučeno navštěvovat příslušnou doménu (viz obrázek níže). 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. Kaspersky Endpoint Security také vytvoří událost o navázání šifrovaného spojení s nedůvěryhodným certifikátem.

V některých případech nemůže aplikace Kaspersky Endpoint Security technicky zobrazit stránku HTML s varováním v prohlížeči (viz obrázek níže), například pokud webový zdroj používá zastaralou verzi síťového protokolu a nestandardní port. V těchto případech Kaspersky Endpoint Security zablokuje přístup k této doméně a prohlížeč zobrazí standardní okno `ERR_CONNECTION_RESET`. Chcete-li získat přístup k webovému zdroji, můžete přidat doménu k výjimkám nebo použít důvěryhodný certifikát.

- Pokud *aplikace nebo služba třetí strany* naváže spojení s doménou s nedůvěryhodným certifikátem, Kaspersky Endpoint Security vytvoří svůj vlastní certifikát pro kontrolu provozu. Nový certifikát má stav *Nedůvěryhodné*. To je nutné pro upozornění aplikace třetí strany na nedůvěryhodné připojení, protože v tomto případě nelze zobrazit stránku HTML a připojení lze navázat v režimu na pozadí. Pokud má tedy aplikace třetí strany integrované nástroje pro ověřování certifikátů, může být připojení ukončeno. V takovém případě musíte kontaktovat vlastníka domény a vytvořit důvěryhodné připojení. Pokud není možné vytvořit důvěryhodné připojení, můžete přidat tuto aplikaci třetí strany do seznamu důvěryhodných aplikací. Kaspersky Endpoint Security také vytvoří událost o navázání šifrovaného spojení s nedůvěryhodným certifikátem.

Jak nakonfigurovat kontrolu šifrovaných připojení s nedůvěryhodným certifikátem v konzole pro správu

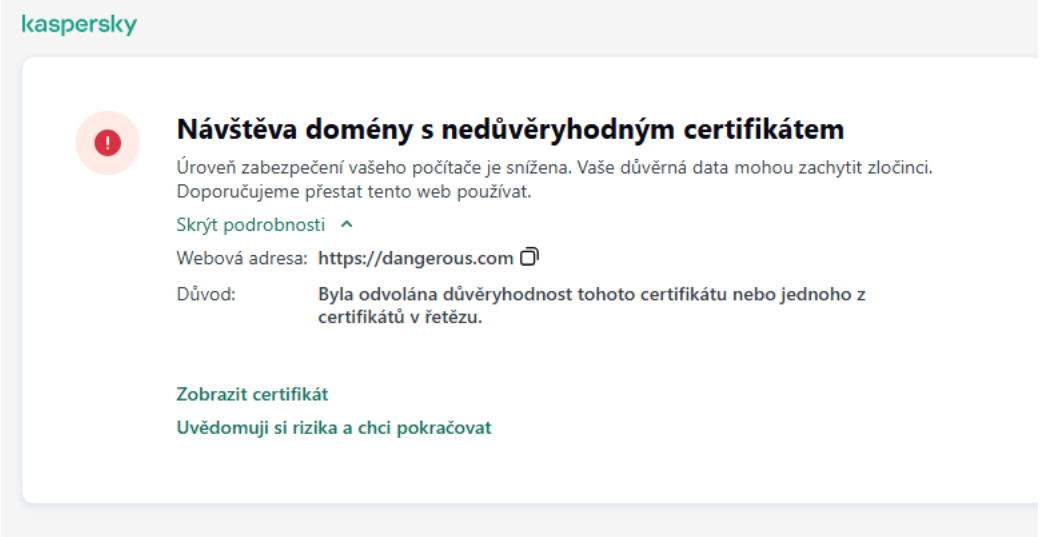
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.
4. V bloku **Kontrola šifrovaných připojení** klikněte na tlačítko **Rozšířené nastavení**.
5. V okně, které se otevře, vyberte provozní režim aplikace při návštěvě domény s nedůvěryhodným certifikátem: **Povolit** nebo **Blokovat**.
6. Uložte změny.

Jak nakonfigurovat kontrolu šifrovaných připojení pomocí nedůvěryhodného certifikátu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. V bloku **Encrypted Connections Scan** klikněte na odkaz **Settings**.
6. V okně, které se otevře, vyberte provozní režim aplikace při návštěvě domény s nedůvěryhodným certifikátem: **Allow connection** nebo **Block connection**.
7. Uložte změny.

Jak nakonfigurovat kontrolu šifrovaných připojení s nedůvěryhodným certifikátem v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.
3. V bloku **Kontrola šifrovaného připojení** vyberte provozní režim aplikace při návštěvě domény s nedůvěryhodným certifikátem: **Povolit** nebo **Blokovat**.
4. Uložte změny.



Upozornění na návštěvu domény s nedůvěryhodným certifikátem

Přidání certifikátu Kaspersky do vlastního úložiště certifikátů

Prohlížeče a poštovní klienti používají k ověření bezpečnosti a pravosti webových zdrojů certifikát. Certifikát také zajišťuje šifrování dat mezi webovými zdroji a uživatelem. Většina prohlížečů a poštovních klientů používá úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Například Google Chrome. Některé prohlížeče a poštovní klienti ve výchozím nastavení namísto úložiště certifikátů Windows používají vlastní úložiště certifikátů. Například Firefox a Thunderbird.

Po instalaci přidá aplikace Kaspersky Endpoint Security certifikát Kaspersky do systémového úložiště důvěryhodných certifikátů (úložiště certifikátů systému Windows). Pokud je ve vaší organizaci nasazena aplikace Kaspersky Security Center a na počítač se používají zásady, aplikace Kaspersky Endpoint Security automaticky povolí používání úložiště certifikátů systému Windows v prohlížečích a poštovních klientech ke kontrole provozu těchto aplikací. Pokud se žádná zásada na počítač nepoužívá, můžete si vybrat úložiště certifikátů, které budou prohlížeče a poštovní klienti používat. Pokud jste vybrali vlastní úložiště certifikátů, přidejte certifikát Kaspersky do úložiště ručně. 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 nekontroluje šifrovaný provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird. Kontrola šifrovaných připojení by měla být povolena také pro kontrolu provozu v poštovních klientech MyOffice Mail a R7-Office Organizer.

Než přidáte certifikát do vlastního úložiště certifikátů prohlížeče nebo poštovního agenta, exportujte certifikát Kaspersky z ovládacího panelu Windows (vlastnosti internetu). Podrobnosti o exportu certifikátu Kaspersky najdete ve znalostní bázi technické podpory. Další informace o přidání certifikátu do obchodu najdete například na webu technické podpory prohlížeče Mozilla.

Úložiště certifikátů si můžete vybrat pouze v místním rozhraní aplikace.

Výběr úložiště certifikátů pro kontrolu šifrovaných připojení v prohlížečích a poštovních klientech:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.
3. V bloku **Kontrola šifrovaného připojení** zaškrtněte políčko **Pokud chcete kontrolovat šifrovaná připojení v aplikacích pomocí jejich vlastního úložiště certifikátů, použijte**.
4. Vyberte úložiště certifikátů:
   - **Úložiště certifikátů Windows (doporučeno)**. Kořenový certifikát společnosti Kaspersky bude přidán do tohoto úložiště během instalace aplikace Kaspersky Endpoint Security.
   - **Vlastní úložiště certifikátů**. 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.

     Poštovní klienti MyOffice Mail a R7-Office Organizer také používají vlastní úložiště certifikátů.
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*. V tomto případě Kaspersky Endpoint Security nekontroluje HTTPS provoz důvěryhodných webových adres, když součásti Ochrana před webovými hrozbami, Ochrana před hrozbami v poště a Kontrola webu vykonávají svoji práci.

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.

Změnu seznamu důvěryhodných adres mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak vyloučit webovou adresu z kontrol šifrovaného připojení v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.
4. V bloku **Kontrola šifrovaných připojení** klikněte na tlačítko **Konfigurovat důvěryhodné adresy**.
5. Klikněte na tlačítko **Přidat**.
6. 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 `*` znak pro zadání masky v názvu domény.

   Aplikace Kaspersky Endpoint Security nepodporuje symbol `*` pro IP adresy. Můžete vybrat rozsah IP adres pomocí masky podsítě (například 198.51.100.0/24).

   Příklady:

   - `domain.com` - záznam obsahuje následující adresy: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Záznam neobsahuje subdomény (např. `subdomain.domain.com`).
   - `subdomain.domain.com` – záznam obsahuje následující adresy: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.
   - `*.domain.com` – záznam obsahuje následující adresy: `https://movies.domain.com`, `https://images.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.
7. Uložte změny.

Jak vyloučit webovou adresu z kontrol šifrovaného připojení ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. V bloku **Encrypted Connections Scan** klikněte na tlačítko **Trusted domains**.
6. Klikněte na tlačítko **Add**.

7. 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 `*` znak pro zadání masky v názvu domény.

   > Aplikace Kaspersky Endpoint Security nepodporuje symbol `*` pro IP adresy. Můžete vybrat rozsah IP adres pomocí masky podsítě (například 198.51.100.0/24).

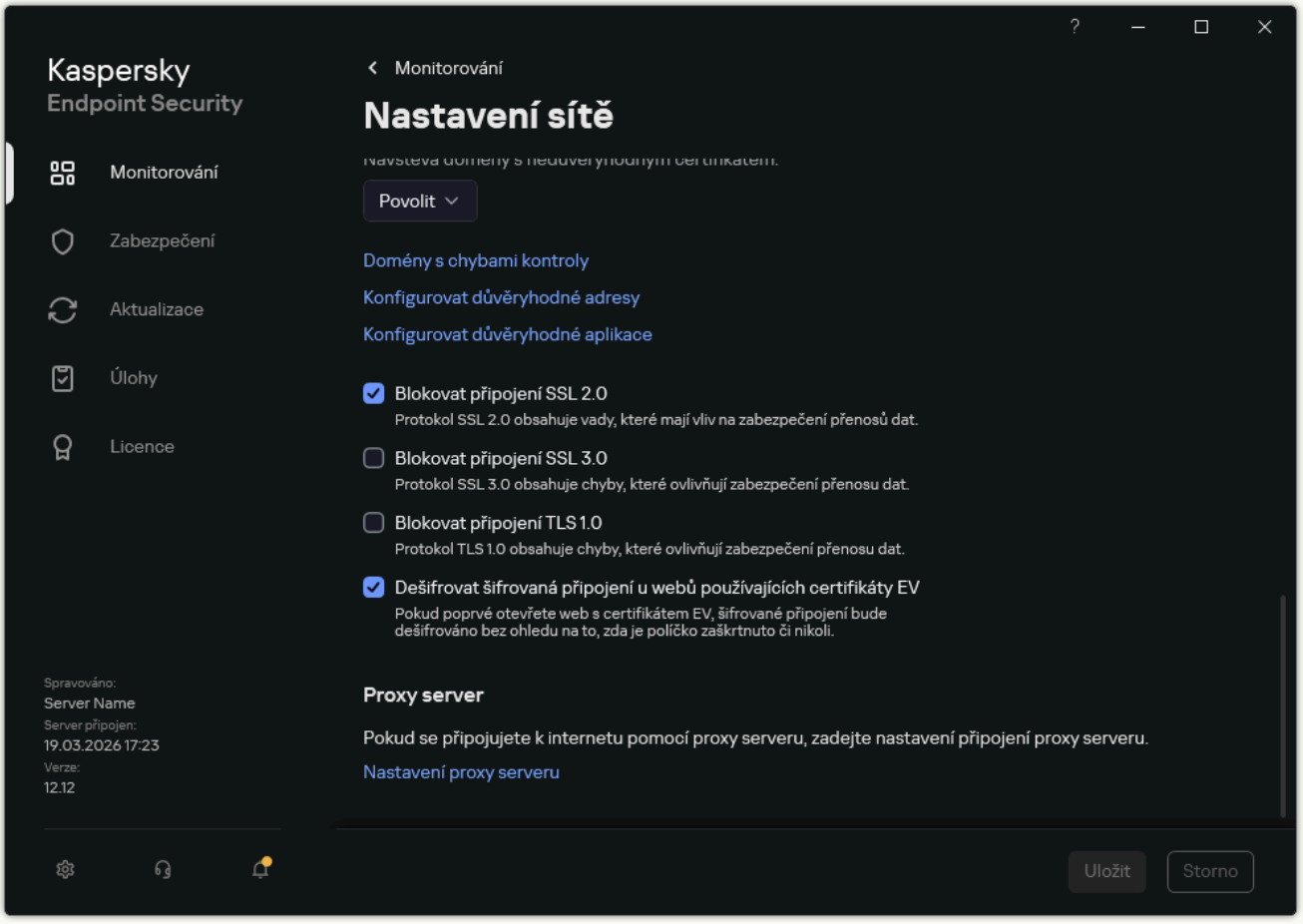
   Příklady:

   - `domain.com` - záznam obsahuje následující adresy: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Záznam neobsahuje subdomény (např. `subdomain.domain.com`).
   - `subdomain.domain.com` – záznam obsahuje následující adresy: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.
   - `*.domain.com` – záznam obsahuje následující adresy: `https://movies.domain.com`, `https://images.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.

8. Uložte změny.

Jak vyloučit webovou adresu z kontrol šifrovaného připojení v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Nastavení sítě**.



Nastavení sítě aplikace

3. V bloku **Kontrola šifrovaného připojení** klikněte na tlačítko **Konfigurovat 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 `*` znak pro zadání masky v názvu domény.

Aplikace Kaspersky Endpoint Security nepodporuje symbol `*` pro IP adresy. Můžete vybrat rozsah IP adres pomocí masky podsítě (například 198.51.100.0/24).

Příklady:

- `domain.com` - záznam obsahuje následující adresy: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Záznam neobsahuje subdomény (např. `subdomain.domain.com`).
- `subdomain.domain.com` – záznam obsahuje následující adresy: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.
- `*.domain.com` – záznam obsahuje následující adresy: `https://movies.domain.com`, `https://images.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.

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.

Zobrazení seznamu domén s chybami kontroly:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.
3. V bloku **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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.
3. V bloku **Kontrola šifrovaného připojení** klikněte na seznam odkazů na důvěryhodné 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.

Výmaz dat

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 *Výmaz dat* 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 *Výmaz 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 konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Wipe data**.

   c. Do pole **Task name** zadejte krátký popis, například *Wipe data (proti krádeži)*.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.

   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. Ukončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

6. Klikněte na úlohu **Wipe data** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

7. Vyberte kartu **Application settings**.

8. Vyberte způsob odstranění dat:

   - **Delete by means of the operating system**. Aplikace Kaspersky Endpoint Security používá prostředky operačního systému k odstranění souborů bez jejich odeslání do koše.
   - **Delete completely, no recovery possible**. Aplikace Kaspersky Endpoint Security přepíše soubory náhodnými daty. Po vymazání je prakticky nemožné obnovit data.

9. Pokud chcete odstranění dat odložit, zaškrtněte políčko **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days**. 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 mějte na paměti, že zaměstnanci mohou mít různou pracovní dobu. 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.

Pokud je počítač vypnutý a připojení není přítomno déle než konfigurovanou dobu, aplikace Kaspersky Endpoint Security po zapnutí počítače neodstraní data okamžitě. Aplikace čeká jednu hodinu na synchronizaci s aplikací Kaspersky Security Center. Je to nutné, aby se zabránilo neoprávněnému odstranění dat na počítačích uživatelů, kteří svůj počítač vypnuli například před odjezdem na dovolenou.

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.
- **Předdefinovaný rozsah**. Aplikace Kaspersky Endpoint Security odstraní soubory z následujících oblastí:
  - **Documents**. Soubory ve standardní systémové složce *Dokumenty* a jejích podsložkách.
  - **Cookies**. Soubory, ve kterých prohlížeč ukládá data z webových stránek navštívených uživatelem (například údaje o autorizaci uživatele).
  - **Desktop**. Soubory ve standardní systémové složce *Plocha* a jejích podsložkách.
  - **Temporary Internet Explorer files**. Dočasné soubory související s provozem aplikace Internet Explorer, jako jsou kopie webových stránek, obrázky a mediální soubory.
  - **Temporary files**. Dočasné soubory související s provozováním aplikací nainstalovaných v počítači. Například aplikace sady Microsoft Office vytvářejí dočasné soubory obsahující záložní kopie dokumentů.
  - **Outlook files**. Soubory související s provozem poštovního klienta aplikace Outlook: datové soubory (PST), offline datové soubory (OST), offline soubory adresáře (OAB) a soubory osobních adresářů (PAB).
  - **User profile**. 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. Uložte změny.
12. Zaškrtněte políčko vedle úlohy.
13. Klikněte na tlačítko **Start**.

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.

Kontrola počítače

Kontrola webu

Součást 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).

Chcete-li používat součást Kontrola webu, musíte provést počáteční konfiguraci aplikace:

- Pro monitorování provozu HTTPS povolte kontrolu šifrovaných připojení (ve výchozím nastavení povolena).
- Vyberte porty, které aplikace Kaspersky Endpoint Security má monitorovat (ve výchozím nastavení aplikace monitoruje všechny porty).
- Vyberte aplikace, jejichž provoz má aplikace Kaspersky Endpoint Security sledovat. Většina prohlížečů se již nachází v seznamu aplikací doporučených společností Kaspersky. Pokud váš prohlížeč v seznamu chybí, přidejte jej ručně.

- Doporučujeme vložit do webového provozu skript interakce s webovou stránkou (ve výchozím nastavení je vkládání skriptů zakázáno). Tento skript umožňuje evidenci událostí součásti Kontrola webu pro protokol událostí aplikace, protokol událostí OS a zprávy.

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 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 „*Grafika*".

- **Jednotlivé adresy**. Můžete zadat webovou adresu nebo použít masky.

Pro regulaci přístupu na webové stránky můžete současně použít několik způsobů. Můžete například omezit přístup k typu dat *Soubory kancelářských aplikací* pouze pro kategorii webu *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.

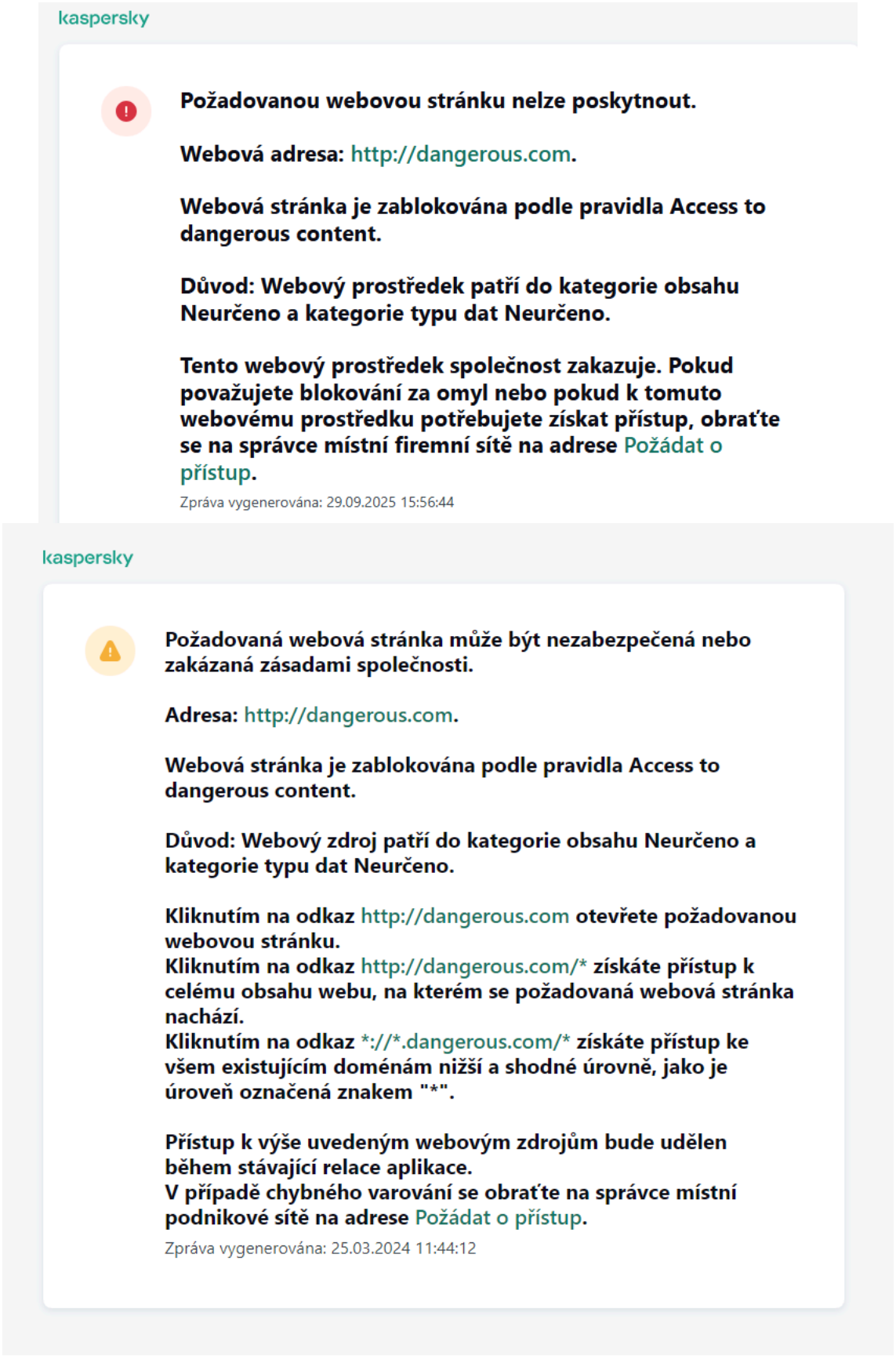
  Můžete například omezit přístup k internetu prostřednictvím prohlížeče pro všechny uživatele společnosti kromě IT oddělení.

- 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

Přidání pravidla přístupu k webovým prostředkům

Pravidlo přístup k webovým prostředkům je soubor filtrů a akcí, které aplikace Kaspersky Endpoint Security používá, když uživatelé navštěvují webové prostředky. Pravidla přístupu mohou zahrnovat plán pravidel.

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. *Výchozí pravidlo* je přednastaveno. 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.

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.

Jak přidat pravidlo přístupu k webovým prostředkům v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.
4. Zaškrtněte políčko **Kontrola webu**.
5. V bloku **Nastavení součásti Kontrola webu** klikněte na tlačítko **Přidat**.

   Otevře se okno **Pravidlo přístupu k webovým prostředkům**.
6. Nakonfigurujte pravidla přístupu k webovým prostředkům (viz tabulka níže).
7. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

   > Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

   Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.
8. Uložte změny.

Jak přidat pravidlo přístupu k webovým prostředkům ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.

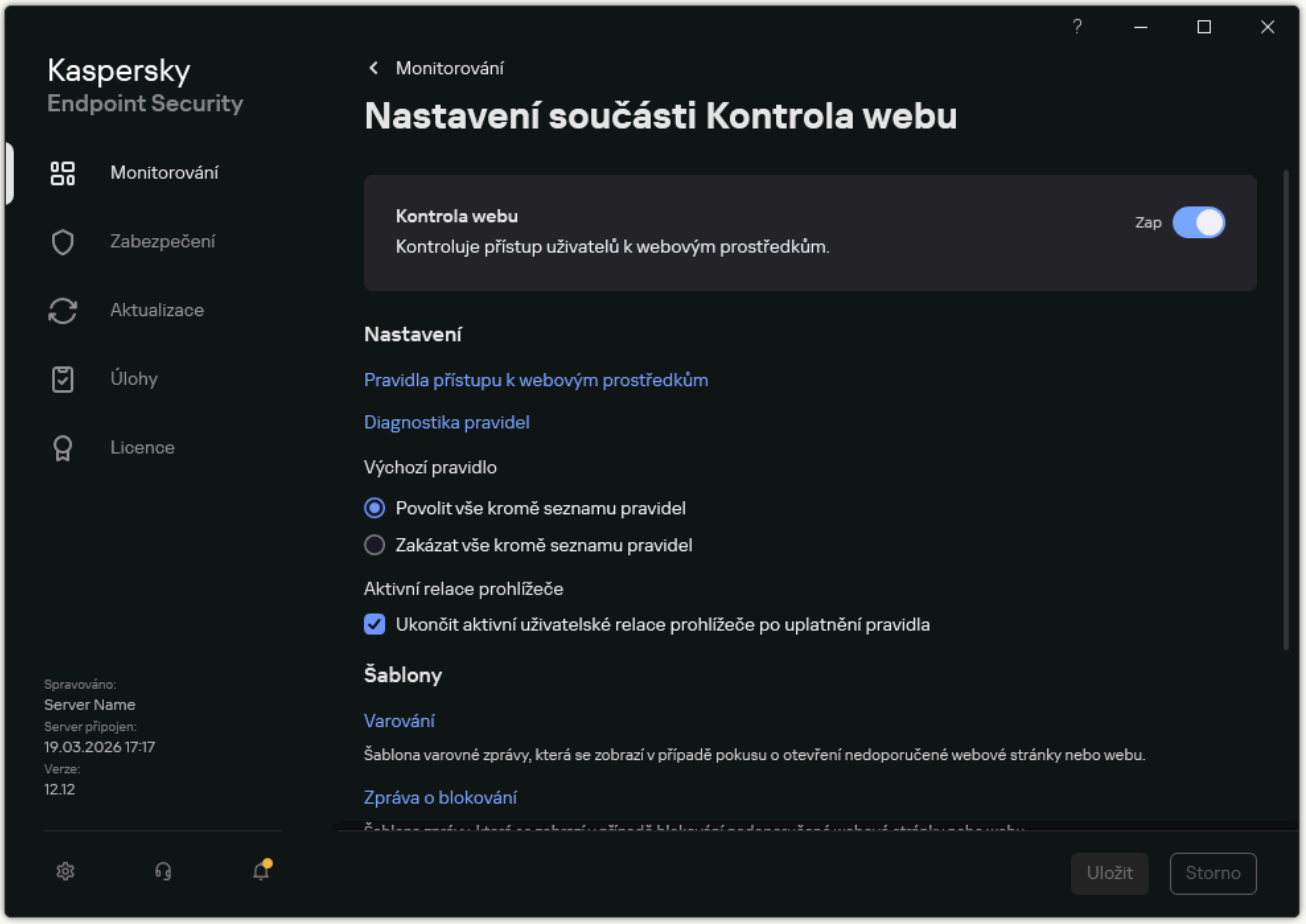
4. Přejděte na **Security Controls** → **Web Control**.
5. Zapněte přepínač **Web Control ENABLED**.
6. V bloku **Rules list** klikněte na tlačítko **Add**.
7. Nakonfigurujte pravidla přístupu k webovým prostředkům (viz tabulka níže).
8. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Terminate active user browser sessions after the rule is applied**.

   Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

   Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.
9. Uložte změny.

Jak přidat pravidlo přístupu k webovým prostředkům v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola webu**.



Nastavení součásti Kontrola webu

3. Zapněte přepínač **Kontrola webu**.
4. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
5. V okně, které se otevře, klikněte na tlačítko **Přidat**.

   Otevře se okno **Pravidlo přístupu k webovým prostředkům**.
6. Nakonfigurujte pravidla přístupu k webovým prostředkům (viz tabulka níže).

7. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

   Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

   Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.

8. Uložte změny.

Nové pravidlo součásti Kontrola webu je přidáno na seznam. V případě potřeby změňte jeho prioritu. Pomocí přepínače můžete pravidlo přístupu k webovým prostředkům také kdykoli zakázat, aniž byste jej ze seznamu odstranili.

Parametry pravidla součásti Kontrola webu

Parametr	Popis
Název pravidla	Název pravidla součásti Kontrola webu.
Stav	• **Zap**. • **Vyp**. Pomocí přepínače můžete kdykoli zakázat pravidlo přístupu k webovým prostředkům.
Akce	• **Povolit**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla. • **Blokovat**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web. • **Varovat**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.
Obsah filtru	• **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 *Grafika*).
Adresy	• **Na všechny adresy**. Kontrola webu nebude filtrovat webové zdroje podle adresy. • **Na jednotlivé adresy**. Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Pokud je zakázána kontrola šifrovaných připojení, v případě protokolu HTTPS můžete filtrovat pouze podle názvu serveru.
Uživatelé	• **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. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
Plán pravidel	Plán pravidla určuje časové rozmezí, během kterého sleduje aplikace Kaspersky Endpoint Security přístup k webovým prostředkům, na které se pravidlo vztahuje. Můžete například omezit přístup k internetu prostřednictvím prohlížeče pouze v pracovní době.

Filtrování podle adres webových prostředků

K řízení přístupu k jednotlivým webovým prostředkům musíte vytvořit pravidlo součásti Kontrola webu, vytvořit seznam webových adres a vybrat akci součásti Kontrola webu. Při vytváření seznamu webových adres můžete zadat adresy URL nebo použít masky.

Pravidla mohou obsahovat plán pravidel a seznam uživatelů, na které se pravidlo vztahuje. Můžete například omezit přístup k webům pouze v pracovní době nebo povolit návštěvu webů uživatelům v určitých skupinách.

Jak povolit filtrování adres webových prostředků v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.
4. Zaškrtněte políčko **Kontrola webu**.
5. V bloku **Nastavení součásti Kontrola webu** klikněte na tlačítko **Přidat**.
   Otevře se okno **Pravidlo přístupu k webovým prostředkům**.
6. Konfigurace pravidla přístupu k webovým prostředkům:
   a. V poli **Název** zadejte název pravidla.
   b. V rozevíracím seznamu **Použít na adresy** vyberte možnost **Na jednotlivé adresy**.
   c. Vytvořte seznam adres webových prostředků. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT.

      Pokud je zakázána kontrola šifrovaných připojení, v případě protokolu HTTPS můžete filtrovat pouze podle názvu serveru.

   d. V rozevíracím seznamu **Použít na uživatele** vyberte příslušný filtr pro uživatele:
      - **Na všechny uživatele**. Kontrola webu nebude filtrovat webové zdroje podle adresy.
      - **Na jednotlivé uživatele nebo skupiny**. Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
   e. V rozevíracím seznamu **Akce** vyberte jednu z možností:
      - **Povolit**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
      - **Blokovat**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.
      - **Varovat**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.
   f. V rozevíracím seznamu **Plán pravidel** vyberte plán nebo vytvořte nový.
7. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

   Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

   Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.
8. Uložte změny.

Jak povolit filtrování adres webových prostředků ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls → Web Control**.

5. Zapněte přepínač **Web Control ENABLED**.

6. V bloku **Rules list** klikněte na tlačítko **Add**.

7. Konfigurace pravidla přístupu k webovým prostředkům:

   a. V poli **Rule name** zadejte název pravidla.

   b. U pravidla přístupu k webovému prostředku vyberte stav **Enabled**.

   Pomocí přepínače můžete pravidlo přístupu k webovým prostředkům kdykoli zakázat, aniž byste jej ze seznamu odstranili.

   c. V bloku **Action** vyberte příslušnou možnost:

   - **Allow**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
   - **Block**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.
   - **Inform**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.

   d. V části **Scope** vyberte možnost **Individual websites**.

   e. Konfigurace filtru obsahu:

   - **Individual address**. Vytvořte seznam adres webových prostředků. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT.

     Pokud je zakázána kontrola šifrovaných připojení, v případě protokolu HTTPS můžete filtrovat pouze podle názvu serveru.

   - **Data type**. Můžete řídit přístup uživatele k webovým prostředkům na základě konkrétního datového typu jeho publikovaných dat (například *Grafika*).

   f. V části **User or group** vyberte uživatele, na které má Kontrola webu pravidlo používat.

   Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

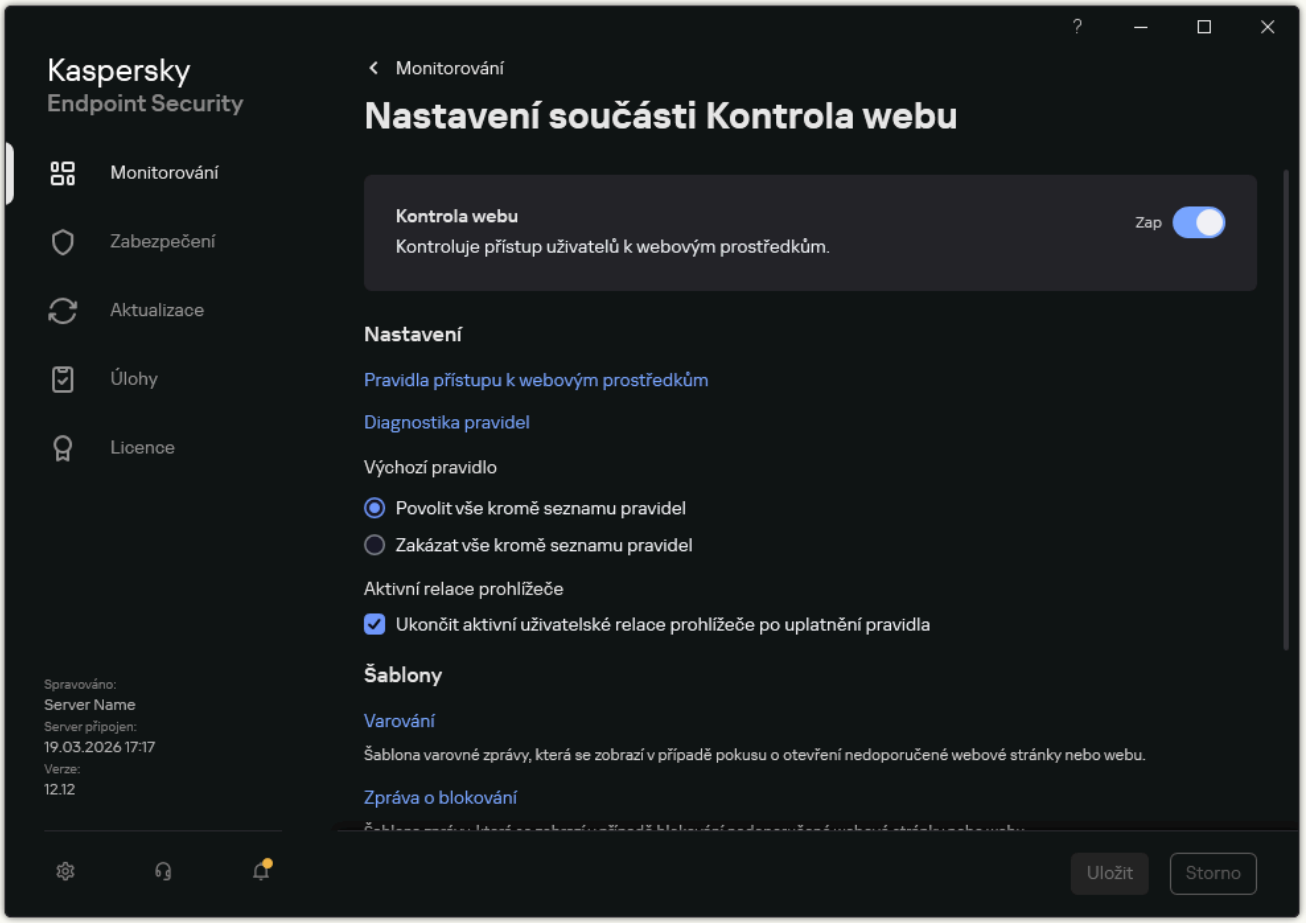
   g. V bloku **Access schedule** vyberte plán nebo vytvořte nový.

8. Uložte změny.

Jak povolit filtrování adres webových prostředků v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola webu**.



Nastavení součásti Kontrola webu

3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
4. V okně, které se otevře, 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 **Zap**.

   Pomocí přepínače můžete kdykoli zakázat pravidlo přístupu k webovým prostředkům.
7. V bloku **Akce** vyberte příslušnou možnost:

   - **Povolit**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
   - **Blokovat**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.
   - **Varovat**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.
8. V části **Adresy** vyberte možnost **Na jednotlivé adresy**.

   Vytvořte seznam adres webových prostředků. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT.

   > Pokud je zakázána kontrola šifrovaných připojení, v případě protokolu HTTPS můžete filtrovat pouze podle názvu serveru.
9. 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 vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

10. V rozevíracím seznamu **Plán pravidel** vyberte plán nebo vytvořte nový.
11. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

    Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

    Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.
12. Uložte změny.

Nové pravidlo součásti Kontrola webu je přidáno na seznam. V případě potřeby změňte jeho prioritu. Pomocí přepínače můžete pravidlo přístupu k webovým prostředkům také kdykoli zakázat, aniž byste jej ze seznamu odstranili.

Filtrování podle obsahu webových prostředků

K řízení přístupu podle obsahu webového prostředku poskytuje součást Kontrola webu filtr kategorií a filtr datových typů.

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.

Můžete omezit přístup uživatelů na web na základě typu dat, například skrýt obrázky. Aplikace Kaspersky Endpoint Security určuje typ dat na základě formátu souboru, a ne na základě jeho přípony. Kontrola webu rozlišuje následující datové typy:

- Video
- Zvuk
- Soubory kancelářských aplikací
- Spustitelné soubory
- Archivy
- Grafika
- Skripty

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 „*Grafika*“.

Pravidla mohou obsahovat plán pravidel a seznam uživatelů, na které se pravidlo vztahuje. Můžete například omezit přístup k webům pouze v pracovní době nebo povolit návštěvu webů uživatelům v určitých skupinách.

Jak povolit filtrování obsahu webových prostředků v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.
4. Zaškrtněte políčko **Kontrola webu**.
5. V bloku **Nastavení součásti Kontrola webu** klikněte na tlačítko **Přidat**.

   Otevře se okno **Pravidlo přístupu k webovým prostředkům**.
6. Konfigurace pravidla přístupu k webovým prostředkům:

   a. V poli **Název** zadejte název pravidla.

   b. V rozevíracím seznamu **Filtrovat obsah** 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 *Grafika*).
- **Podle kategorií obsahu a typů dat**. Jsou povoleny filtry podle kategorií obsahu a typů dat.

Po výběru filtrů nakonfigurujte jejich parametry.

c. V rozevíracím seznamu **Použít na uživatele** vyberte příslušný filtr pro uživatele:

- **Na všechny uživatele**. Kontrola webu nebude filtrovat webové zdroje podle adresy.
- **Na jednotlivé uživatele nebo skupiny**. Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

d. V rozevíracím seznamu **Akce** vyberte jednu z možností:

- **Povolit**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
- **Blokovat**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.
- **Varovat**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.

e. V rozevíracím seznamu **Plán pravidel** vyberte plán nebo vytvořte nový.

7. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.

8. Uložte změny.

Jak povolit filtrování obsahu webových prostředků ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Web Control**.
5. Zapněte přepínač **Web Control ENABLED**.
6. V bloku **Rules list** klikněte na tlačítko **Add**.
7. Konfigurace pravidla přístupu k webovým prostředkům:

   a. V poli **Rule name** zadejte název pravidla.

   b. U pravidla přístupu k webovému prostředku vyberte stav **Enabled**.
   Pomocí přepínače můžete kdykoli zakázat pravidlo přístupu k webovým prostředkům.

   c. V bloku **Action** vyberte příslušnou možnost:

   - **Allow**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
   - **Block**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.

- **Inform**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.

d. V části **Scope** vyberte možnost **Content category**.

e. Konfigurace filtru obsahu:

- **Content category**. Přístup uživatelů k webovým prostředkům můžete ovládat podle kategorie (například kategorie *Sociální sítě*).
- **Data type**. Můžete řídit přístup uživatele k webovým prostředkům na základě konkrétního datového typu jeho publikovaných dat (například *Grafika*).

f. V části **User or group** vyberte uživatele, na které má Kontrola webu pravidlo používat.

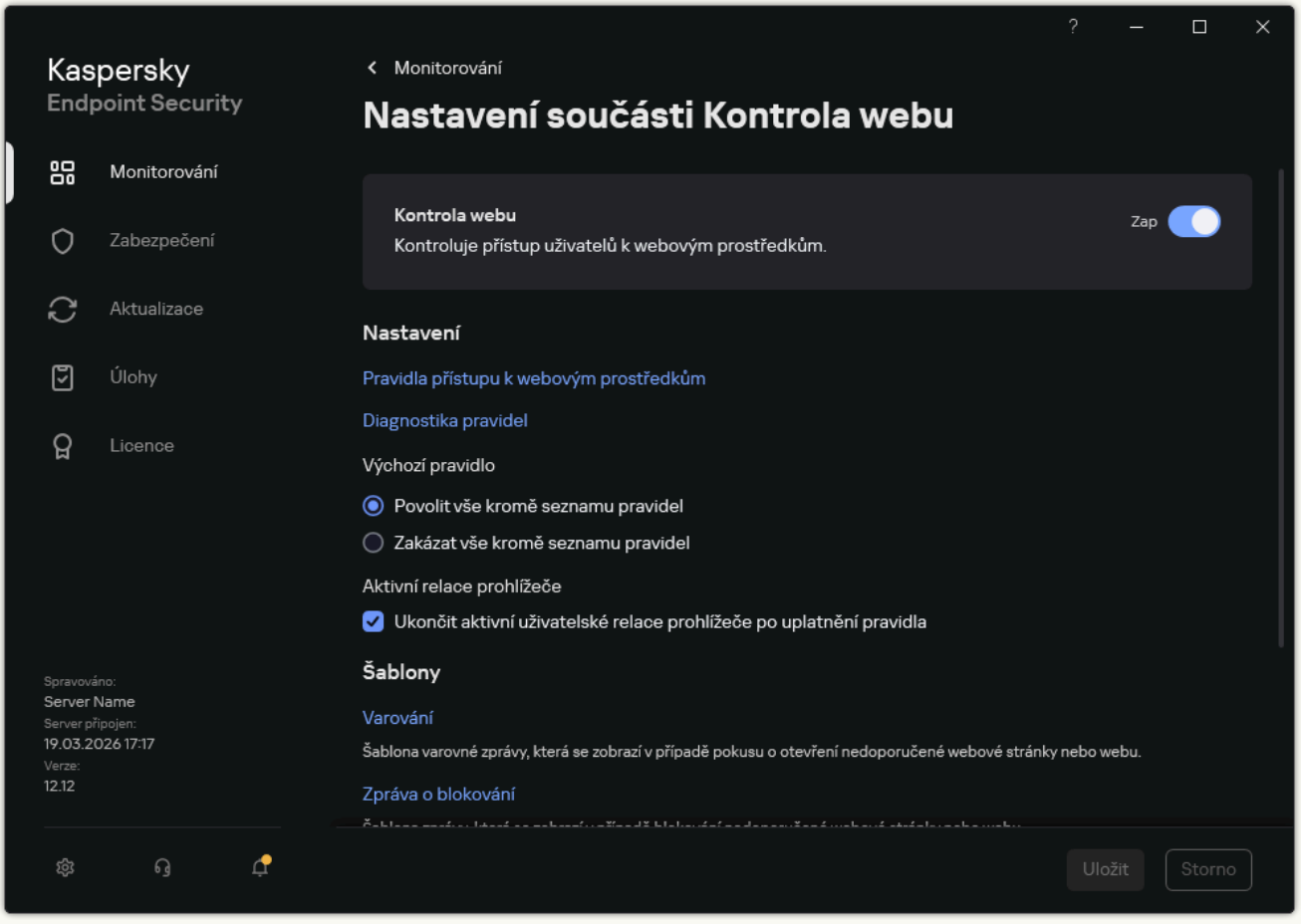
Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

g. V bloku **Access schedule** vyberte plán nebo vytvořte nový.

8. Uložte změny.

Jak povolit filtrování obsahu webových prostředků v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola webu**.



Nastavení součásti Kontrola webu

3. V bloku **Nastavení** klikněte na tlačítko **Pravidla přístupu k webovým prostředkům**.
4. V okně, které se otevře, 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 **Zap**.

   Pomocí přepínače můžete kdykoli zakázat pravidlo přístupu k webovým prostředkům.

7. V bloku **Akce** vyberte příslušnou možnost:

   - **Povolit**. Kontrola webu umožní přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla.
   - **Blokovat**. Kontrola webu zablokuje přístup k webovým prostředkům, které vyhovují pravidlům příslušného pravidla, a zobrazí zprávu o odepření přístupu na web.
   - **Varovat**. Když se uživatel pokusí získat přístup k webovému zdroji, který vyhovuje příslušnému pravidlu, zobrazí součást Kontrola webu varování, že návštěva webového zdroje není vhodná. Pomocí odkazů ve varování může uživatel získat přístup k požadovanému webovému prostředku.

8. V bloku **Obsah 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 *Grafika*).

   Postup konfigurace filtru obsahu:

   a. Klikněte na odkaz **Nastavení**.

   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 **Uživatelé** vyberte příslušný filtr pro uživatele:

   - **Na všechny uživatele**. Kontrola webu nebude filtrovat webové zdroje podle adresy.
   - **Na jednotlivé uživatele a/nebo skupiny**. Kontrola webu vyfiltruje ze seznamu pouze adresy webových zdrojů. Můžete zadat webovou adresu nebo použít masky. Můžete také exportovat seznam adres webových prostředků ze souboru TXT. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Vytvoření seznamu uživatelů, na které chcete pravidlo použít:

     a. Klikněte na tlačítko **Přidat**.

     b. V okně, které se otevře, vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo přístupu k webovému prostředku.

     c. Vraťte se do okna pro konfiguraci pravidla přístupu k webovým prostředkům.

10. V rozevíracím seznamu **Plán pravidel** vyberte název požadovaného plánu nebo vygenerujte nový plán na základě vybraného plánu pravidla. Postup:

    a. Klikněte na tlačítko **Upravit nebo přidat nový**.

    b. V okně, které se otevře, 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.

11. Pokud chcete, aby součást Kontrola webu ukončila připojení k zakázaným webovým zdrojům okamžitě po použití zásady, zaškrtněte políčko **Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla**.

    Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

    Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.

12. Uložte změny.

Nové pravidlo součásti Kontrola webu je přidáno na seznam. V případě potřeby změňte jeho prioritu. Pomocí přepínače můžete pravidlo přístupu k webovým prostředkům také kdykoli zakázat, aniž byste jej ze seznamu odstranili.

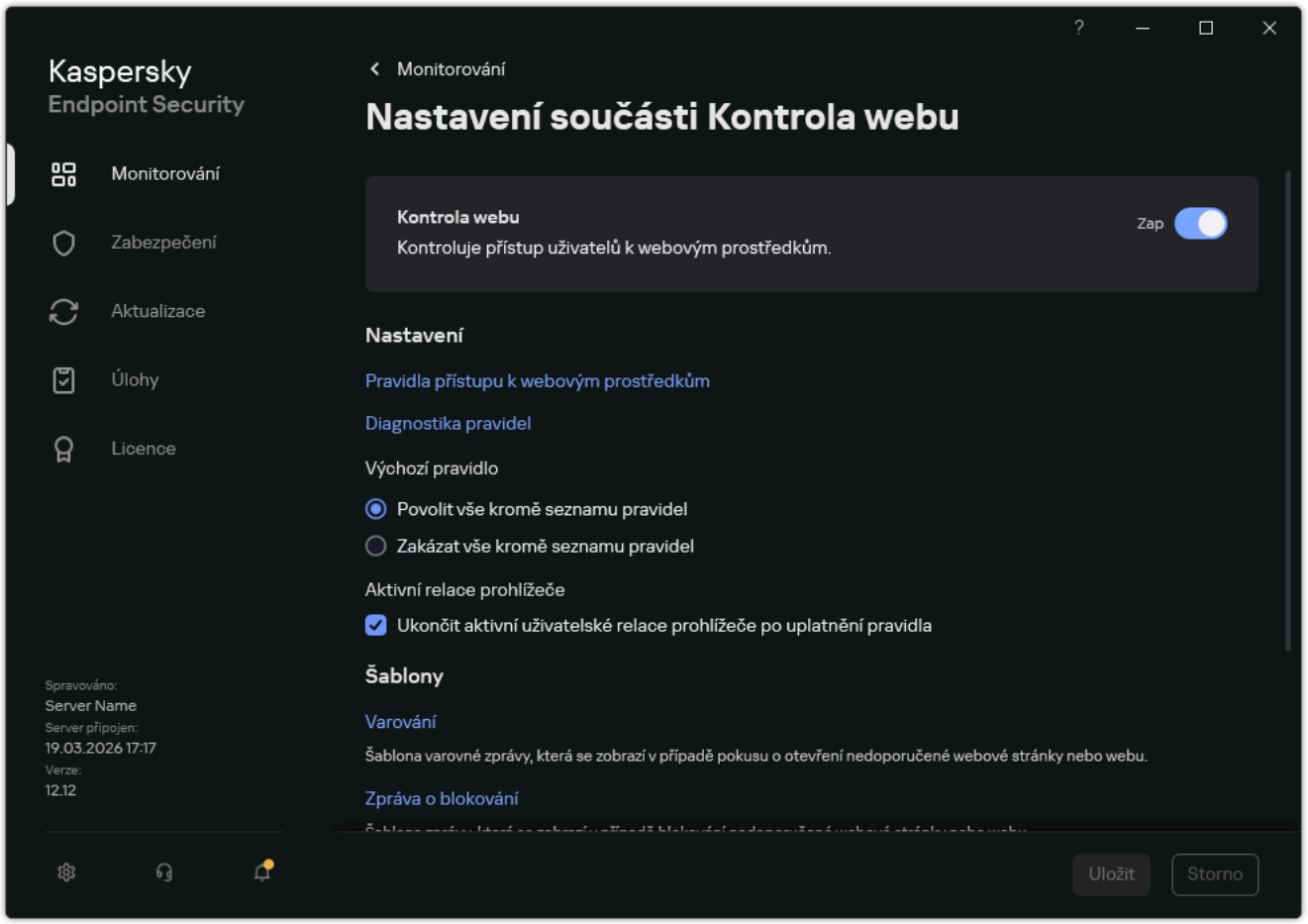
Testování pravidel přístupu k webovým prostředkům

Při konfiguraci součásti Kontrola webu můžete nechtěně zablokovat přístup k webovým prostředkům, které uživatelé potřebují k práci. Pro zjištění, jaké pravidlo součásti Kontrola webu blokuje přístup k webovým prostředkům, můžete použít nástroj *Diagnostika pravidel součásti Kontrola webu*. Diagnostika pravidel součásti Kontrola webu je k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security. V konzole aplikace Kaspersky Security Center nelze zjistit, které pravidlo součásti Konzola zahrnuje daný 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.

Postup testování pravidel přístupu k webovým prostředkům:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola webu**.



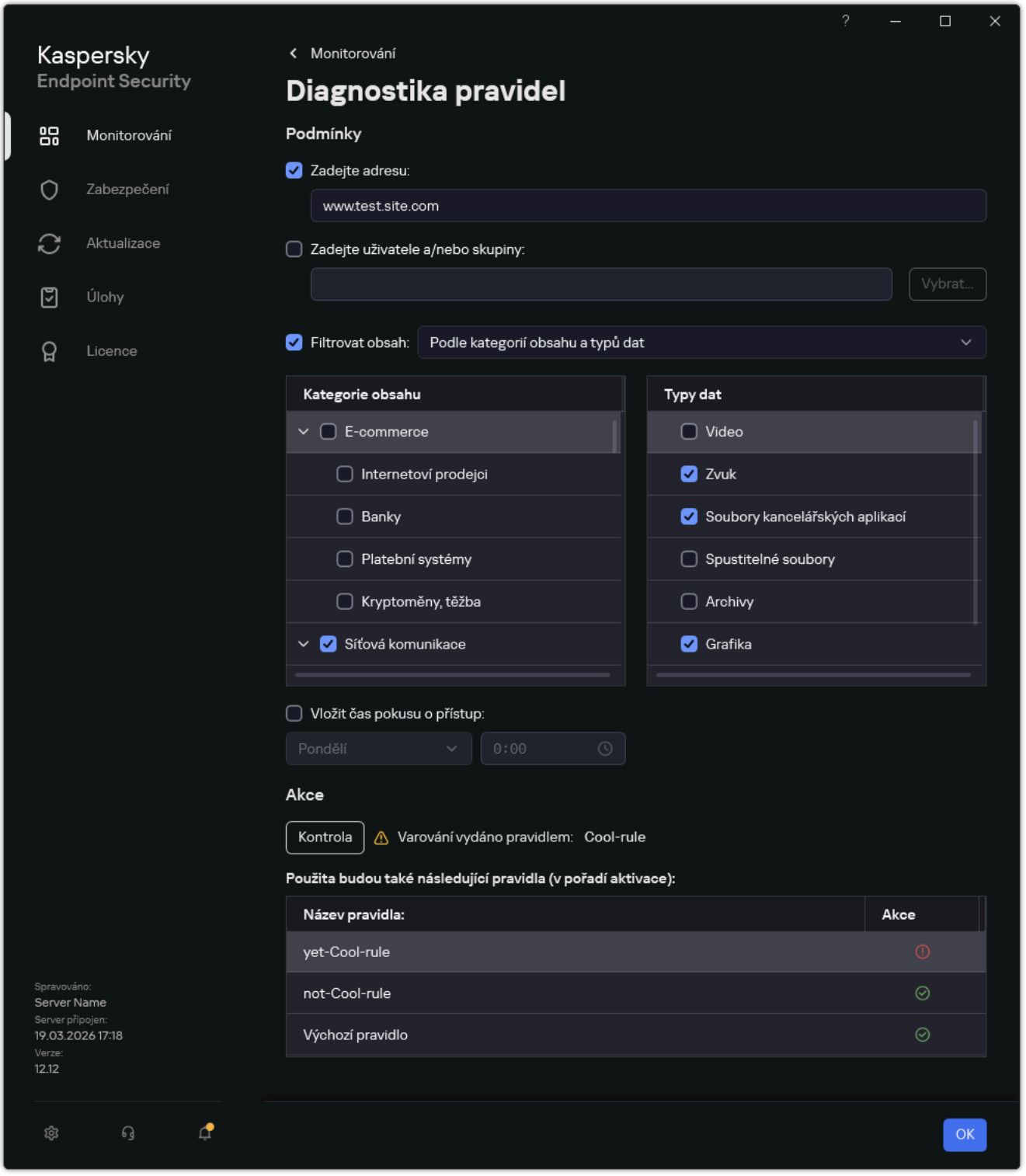
Nastavení součásti Kontrola webu

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 s určitými 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 **Kontrola**.

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 (povolení, blokování nebo varování). 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 **Kontrola**.
V následující tabulce jsou uvedena zbývající aktivovaná pravidla společně s akcí prováděnou aplikací Kaspersky Endpoint Security. Pravidla jsou uvedena v pořadí podle sestupné priority.



Výsledek testu přístupu k webovým prostředkům

Export a import pravidel součásti Kontrola webu

Seznam pravidel součásti Kontrola webu můžete exportovat do souboru XML nebo JSON. Pak můžete soubor upravit, například přidat velké množství adres stejného typu. Můžete použít funkci exportu/importu k zálohování seznamu pravidel součásti Kontrola webu nebo k migraci seznamu na jiný server.

[Jak exportovat a importovat seznam pravidel součásti Kontrola webu v konzole pro správu (MMC)]

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.

4. Postup exportu seznamu pravidel součásti Kontrola webu:

   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. Uložte soubor.

   Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.

5. Postup importu seznamu pravidel součásti Kontrola webu:

   a. Klikněte na odkaz **Importovat**.

   V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.

   b. Otevřete soubor.

   Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

6. Uložte změny.

Jak exportovat a importovat seznam pravidel součásti Kontrola webu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls** → **Web Control**.

5. Postup exportu seznamu pravidel v bloku **Rules list**:

   a. Vyberte pravidla, která chcete exportovat.

   b. Klikněte na tlačítko → **Export**.

   Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru JSON ve výchozí složce pro stahování.

6. Postup importu seznamu pravidel v bloku **Rules list**:

   a. Klikněte na tlačítko → **Import**.

   V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam pravidel.

   b. Otevřete soubor.

   Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.

7. Uložte změny.

Export a import adres webových prostředků pravidla Kontrola webu

Pokud jste vytvořili seznam adres webových prostředků v pravidle přístupu k webovým prostředkům, můžete jej exportovat do souboru:

- Ve formátu TXT v konzole pro správu (MMC)
- Ve formátu CSV v rozhraní aplikace

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.

Můžete také exportovat/importovat všechna pravidla součásti Kontrola webu, a ne pouze adresy webových prostředků jednotlivých pravidel.

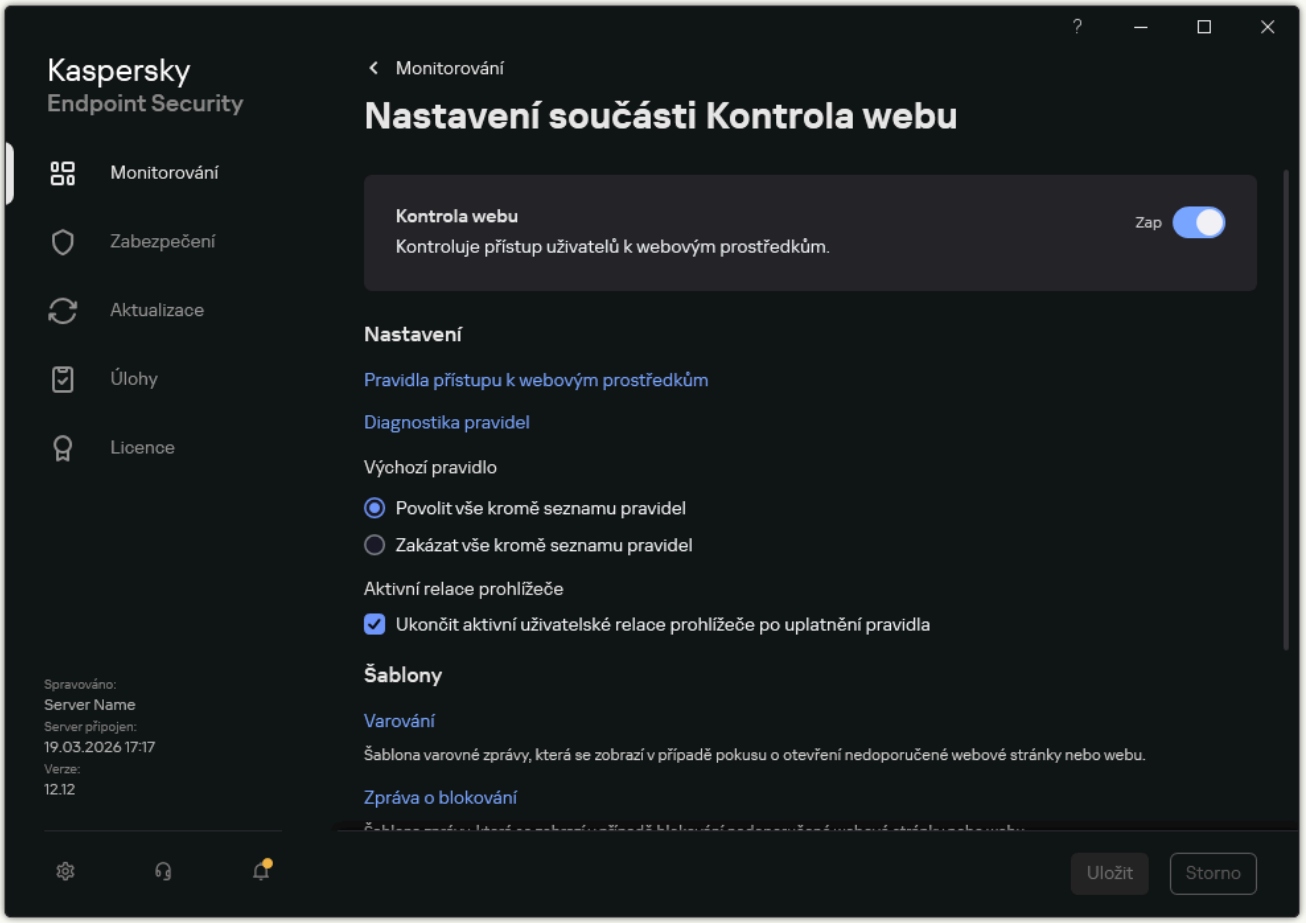
Adresy webových prostředků pravidla součásti Kontrola webu nemůžete exportovat/importovat ve webové konzole ani cloudové konzole.

Jak exportovat/importovat adresy webových prostředků pravidla součásti Kontrola webu v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.
4. V bloku **Nastavení součásti Kontrola webu** vyberte pravidlo, jehož seznam adres webových prostředků chcete exportovat nebo importovat.
   Zobrazují se pravidla součásti Kontrola webu.
5. Chcete-li exportovat seznam webových prostředků, proveďte v seznamu adres následující akce:
   a. Vyberte adresy, které chcete exportovat.
      Pokud jste nevybrali žádnou adresu, aplikace Kaspersky Endpoint Security exportuje všechny adresy.
   b. Klikněte na tlačítko .
   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. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje seznam adres webových prostředků do souboru TXT.
6. Chcete-li importovat seznam webových prostředků, proveďte v seznamu adres následující akce:
   a. Klikněte na tlačítko .
      V okně, které se otevře, vyberte soubor TXT, ze kterého chcete importovat seznam webových prostředků.
   b. Otevřete soubor.
      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.

Jak exportovat/importovat adresy webových prostředků pravidla součásti Kontrola webu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola webu**.



Nastavení součásti 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 CSV, do kterého chcete exportovat seznam důvěryhodných adres webových prostředků, a vyberte složku, do které chcete tento soubor uložit.
   d. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje seznam adres webových prostředků do souboru CSV.
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 CSV, ze kterého chcete importovat seznam webových prostředků.
   b. Otevřete soubor.
      Pokud počítač již seznam adres obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru CSV 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.

Prohlížeče podporující funkci monitorování: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorování aktivity uživatele v jiných prohlížečích nefunguje.

Aplikace Kaspersky Endpoint Security vytváří následující události aktivity uživatele na internetu:

- Blokovat web (stav *Critical*).
- Návštěva nedoporučeného webu (Stav *Warning*).
- Návštěva povolených webových stránek (stav *Info*).

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.

Vložení skriptu interakce s webovou stránkou

Jak vložit skript interakce s webovou stránkou do webového provozu v konzole pro správu (MMC)

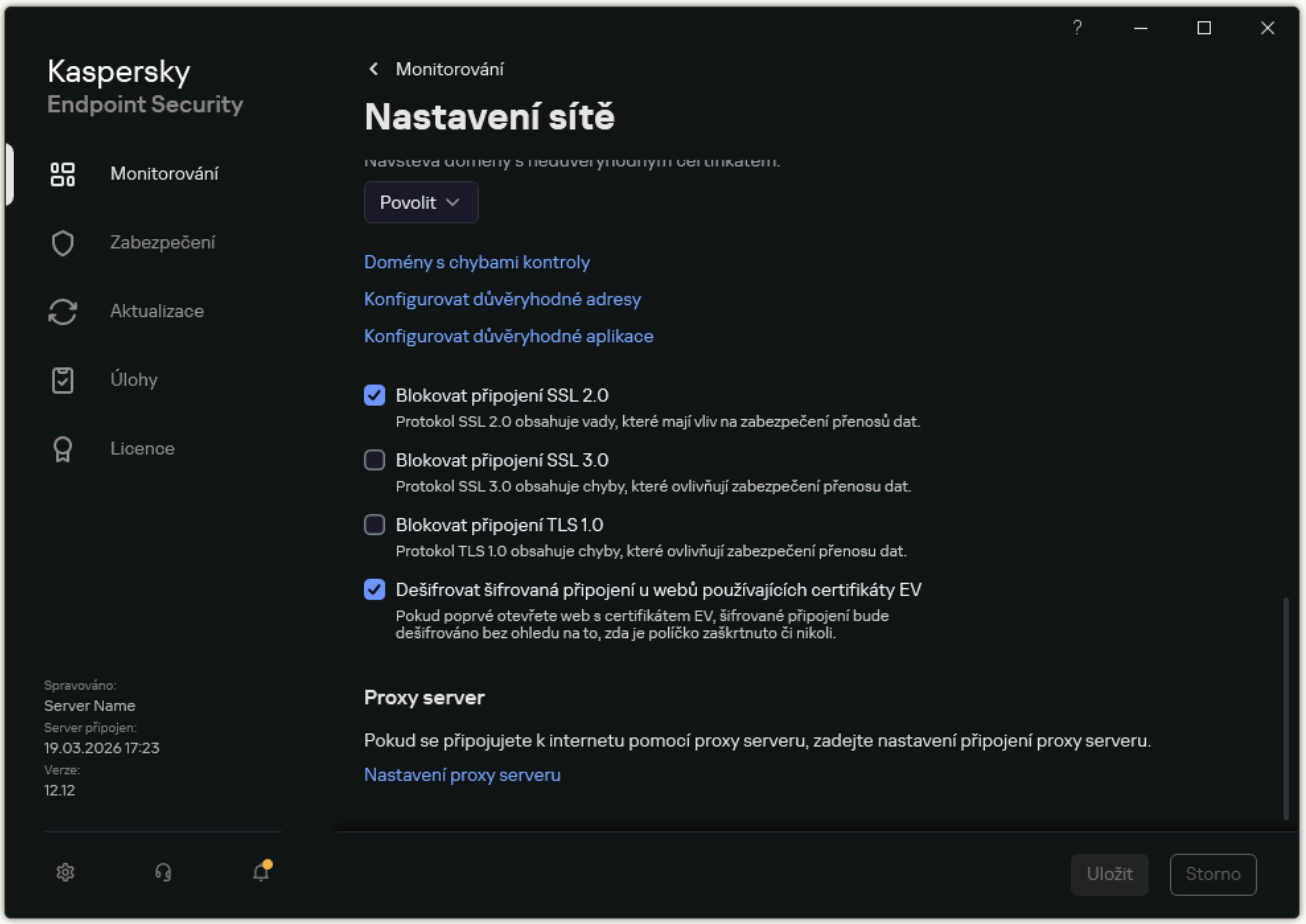
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.
4. V bloku **Kontrola šifrovaných připojení** zaškrtněte políčko **Vkládat skript do síťového provozu za účelem interakce s webovými stránkami**.
5. Uložte změny.

Jak vložit skript interakce s webovou stránkou do webového provozu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. V okně zásad vyberte **General Settings** → **Network Settings**.
5. V části **Monitoring of internet connections** zapněte přepínač **Monitoring of internet connections ENABLED**.
6. Uložte změny.

Jak vložit skript interakce s webovou stránkou do webového provozu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.



Nastavení sítě aplikace

3. V bloku **Zpracování provozu** zaškrtněte políčko **Vkládat skript do síťového provozu za účelem interakce s webovými stránkami**.

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.

Konfigurace protokolování událostí součásti Kontrola webu

Postup konfigurace protokolování událostí součásti Kontrola webu v počítači uživatele:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Rozhraní**.

3. V bloku **Upozornění** klikněte na tlačítko **Konfigurovat 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:

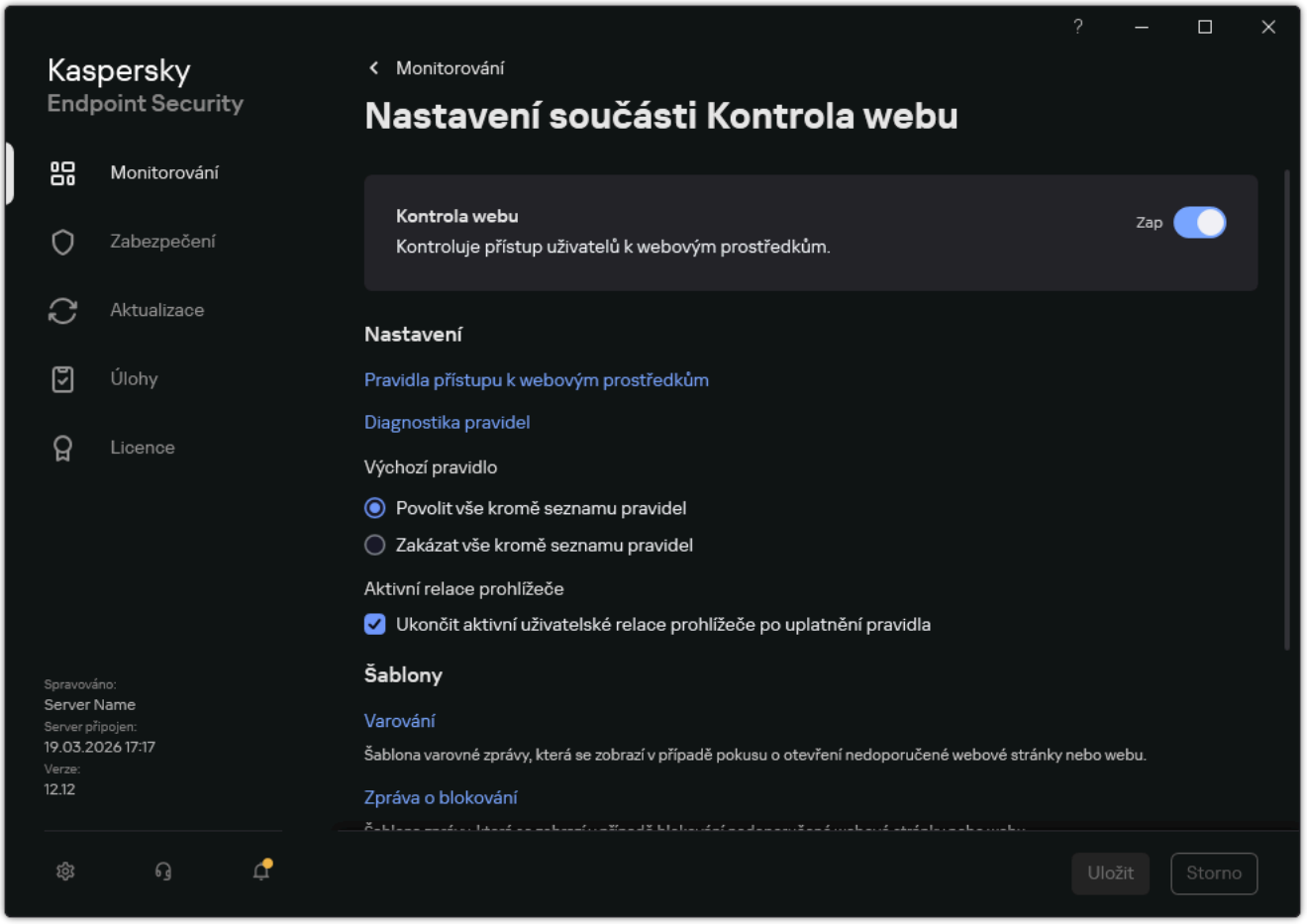
- Pokud používáte aplikaci Kaspersky Security Center, součást Kontrola webu odešle události pro všechny objekty, které tvoří webovou stránku. Z tohoto důvodu může být v případě, že je jeden web blokovaný, vytvořeno více událostí. Například při blokování webu http://www.example.com může aplikace Kaspersky Endpoint Security předávat události pro následující objekty: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.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.example.com/main, http://www.example.com/contact, http://www.example.com/gallery, aplikace Kaspersky Endpoint Security odešle pouze jednu událost s objektem http://www.example.com.

Protokolování událostí při návštěvě povolených webů

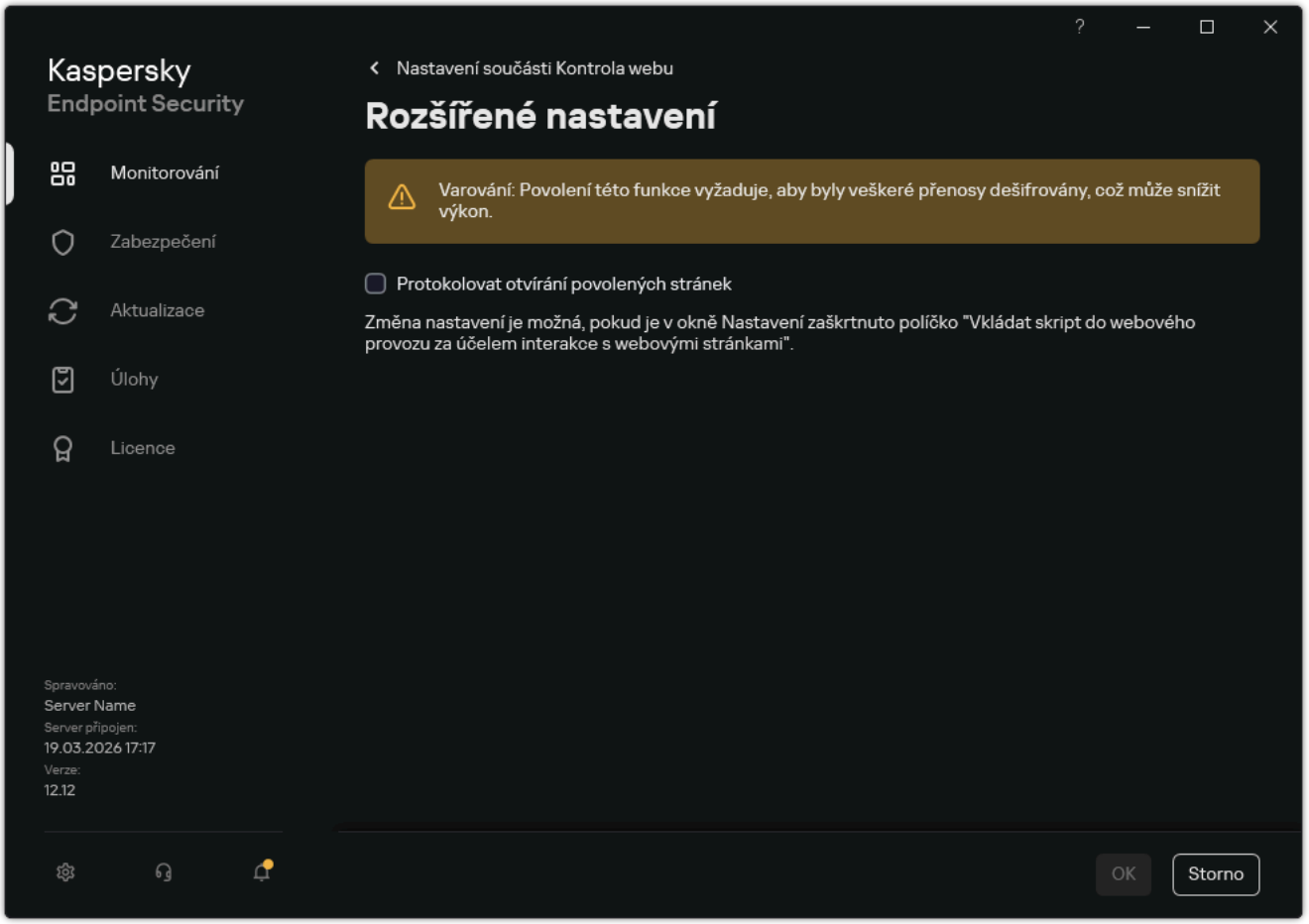
Postup povolení protokolování událostí při návštěvě povolených webů:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola webu**.



Nastavení součásti Kontrola webu

3. V bloku **Další** klikněte na tlačítko **Rozšířené nastavení**.
4. V okně, které se otevře, zaškrtněte políčko **Protokolovat otvírání povolených stránek**.



Rozšířené nastavení součásti Kontrola webu

5. Uložte změny.

Díky tomu budete moci zobrazit celou historii prohlížeče.

Úprava šablon zpráv součásti Kontrola webu

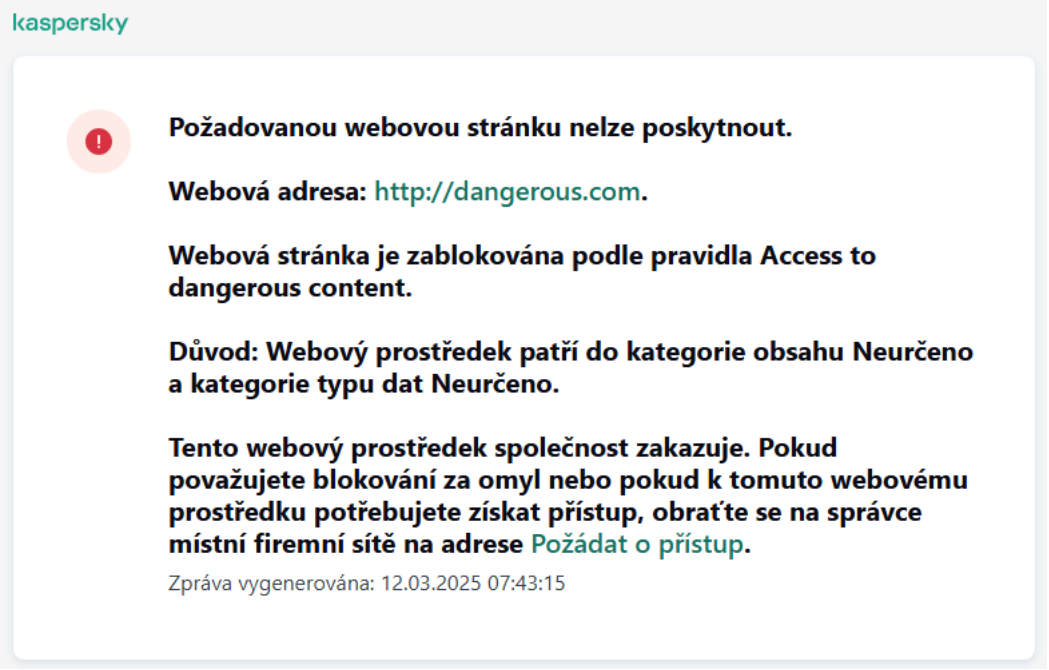
V závislosti na typu akce zadané ve vlastnostech pravidel součásti Kontrola webu zobrazí aplikace Kaspersky Endpoint Security zprávu jednoho z následujících typů, když se uživatel pokusí o přístup k internetovým zdrojům (aplikace nahradí stránku HTML zprávou pro odpověď serveru HTTP):

- 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 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 (viz obrázek níže), pokud je v nastavení pravidla, které popisuje daný webový prostředek, vybrána možnost **Blokovat**.

  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.



Zpráva o blokování webových zdrojů

Pro varovnou zprávu, zprávu s informací o zablokování webového prostředku a zprávu odesílanou správci sítě LAN jsou k dispozici zvláštní šablony. Pro správu šablon zprávy jsou k dispozici speciální proměnné (např. `%USER_NAME%`). Proměnné umožňují použití jedné šablony zprávy pro různé počítače. Při generování zprávy aplikace Kaspersky Endpoint Security načte hodnotu proměnné z nastavení operačního systému a vloží ji do zprávy odpovídající konkrétnímu počítači, uživateli a události.

Jak změnit šablonu zprávy součásti Kontrola webu v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola webu**.
4. V bloku **Nastavení šablony zprávy** klikněte na tlačítko **Šablony**.
5. Nakonfigurujte šablony zpráv 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.
   - **Zpráva o blokování**. Pole pro zadání obsahuje šablonu zprávy, která se zobrazí, pokud je aktivováno pravidlo, které blokuje přístup k webovému prostředku.
   - **Zpráva pro správce**. Šablona zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k webové stránce určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Proměnná** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Výchozí text šablony můžete také obnovit pomocí tlačítka **Výchozí režim**.
6. Uložte změny.

Jak změnit šablonu zprávy součásti Kontrola webu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls** → **Web Control**.

5. V bloku **Message templates** klikněte na odkaz **Message about website blocking** a nakonfigurujte šablony pro zprávy součásti Kontrola webu:

   - **Warning**. Pole pro zadání zahrnuje šablony zprávy, která se zobrazí, pokud je aktivováno pravidlo varování o pokusech o přístup k nežádoucímu webovému prostředku.
   - **Message about blocking**. Pole pro zadání obsahuje šablonu zprávy, která se zobrazí, pokud je aktivováno pravidlo, které blokuje přístup k webovému prostředku.
   - **Message to administrator**. Šablona zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k webové stránce určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Add variable** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

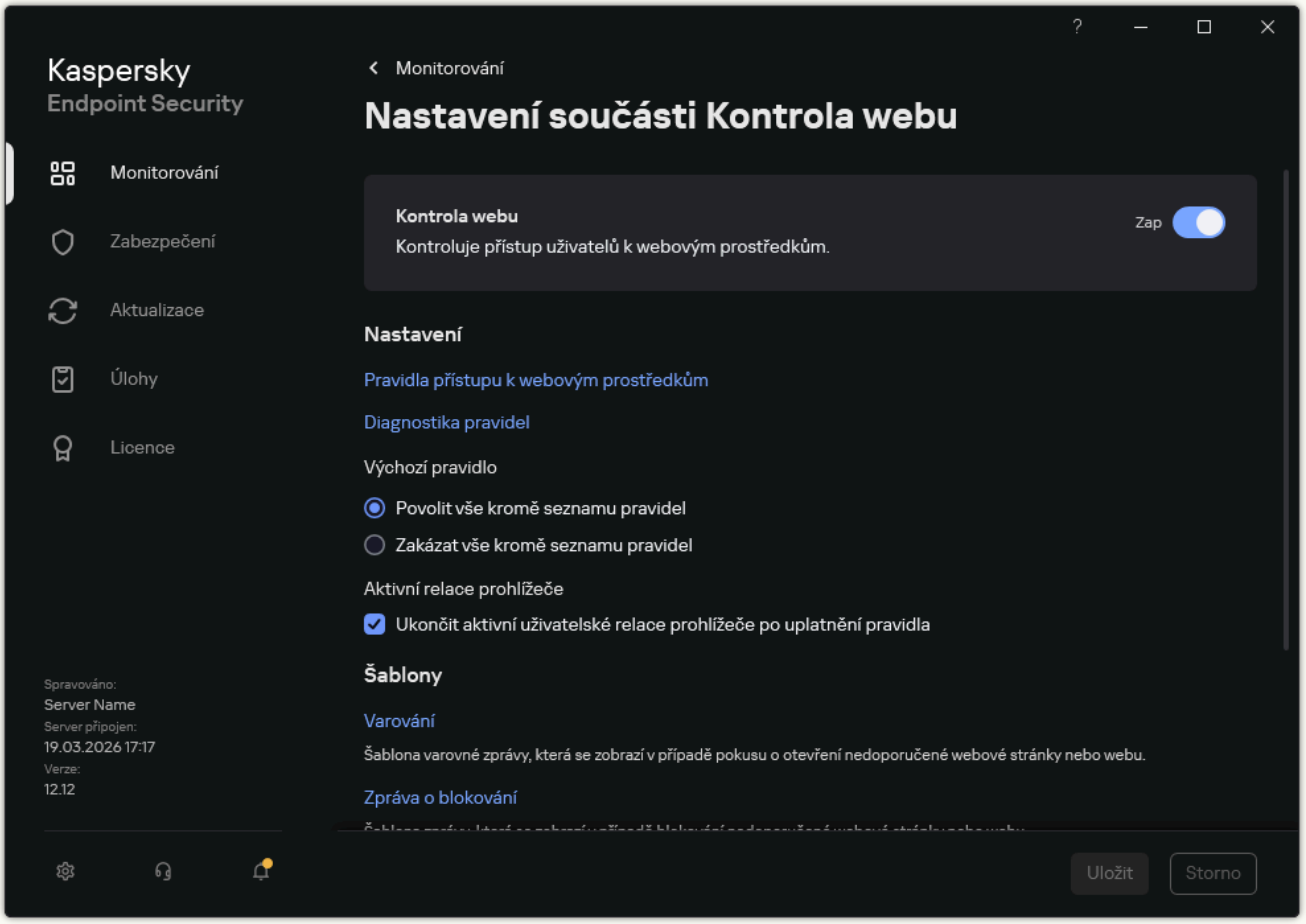
   Výchozí text šablony můžete také obnovit pomocí tlačítka **Reset to default**.

6. Uložte změny.

Jak změnit šablonu zprávy součásti Kontrola webu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola webu**.



Nastavení součásti 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.

- **Zpráva o blokování**. Pole pro zadání obsahuje šablonu zprávy, která se zobrazí, pokud je aktivováno pravidlo, které blokuje přístup k webovému prostředku.

- **Zpráva správci**. Šablona zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k webové stránce určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Přidat proměnnou** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

Výchozí text šablony můžete také obnovit pomocí tlačítka **Obnovit**.

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.example.com/page_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 `*.example.com` představuje následující adresy:

   - `http://pictures.example.com`. Maska domény `*.` představuje `pictures.`
   - `http://user.pictures.example.com`. Maska domény `*.` představuje `pictures.` a `user.`
   - `http://example.com`. Maska domény `*.` je interpretován jako prázdný řádek

3. Sekvence znaků `www.` na začátku masky adresy je interpretována jako sekvence `*.`.

   Příklad: Maska adresy `www.example.com` je zpracována jako `*.example.com`. Tato maska pokrývá adresy `www2.example.com` a `www.pictures.example.com`.

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.example.com` zahrnuje adresy jako například `http://www.example.com/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 `example.com` zahrnuje adresy `http://example.com` a `https://example.com`.

   - 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://*.example.com` zahrnuje adresu `http://www.example.com`, ale nezahrnuje adresu `https://www.example.com`.

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.example.com	http://www.example.com	Ano	Viz pravidla 3, 2, 1.
7	www.example.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.example.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 pravidlo 6.
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.example.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.example.com/*"	http://www.example.com/abc	Ano	Viz pravidly 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.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.

Kontrola webu pro virtuální počítače

Kontrola webu řídí provoz v počítači i na virtuálním počítači, který je lokálně nasazen v počítači. Funguje to bez nutnosti instalace aplikace Kaspersky Endpoint Security na místní virtuální počítač. To znamená, že pokud se uživatel pokusí v součásti na *virtuálním počítači* otevřít web, který je blokován pravidlem součásti Kontrola webu, aplikace nainstalovaná v hostitelském operačním systému *počítače* odepře přístup na tento web.

Kontrola webu funguje na různých virtuálních počítačích odlišně.

Oracle VM VirtualBox

Kaspersky Endpoint Security podporuje pravidla součásti Kontrola webu na virtuálních počítačích Oracle VM VirtualBox bez omezení. Aplikace může řídit veškerý provoz virtuálního počítače. Pokud je v pravidlech součásti Kontrola webu nakonfigurován filtr podle uživatele, aplikace funguje správně, protože všechny procesy virtuálních počítačů spouští místní uživatel.

VMware Workstation

Kaspersky Endpoint Security podporuje pravidla součásti na virtuálních počítačích VMware Workstation s omezeními. Aplikace nepodporuje pravidla s filtrem nakonfigurovaným uživatelem. Procesy virtuálního počítače běží pod uživatelem system (SYSTEM). To znemožňuje identifikaci uživatele, který se pokouší otevřít webovou stránku na virtuálním počítači.

Microsoft Hyper-V

Kaspersky Endpoint Security nepodporuje pravidla součásti Kontrola webu na virtuálních počítačích Microsoft Hyper-V.

Proměnné v šablonách zpráv součásti Kontrola webu

V šablonách zpráv uživatelů nebo šablon zpráv správce můžete použít následující proměnné:

- **User** – `%USER_NAME%`.

  Název aktuálního uživatelského účtu v počítači, na kterém byla zpráva vygenerována, ve formátu `<device name>\<user alias>` (např. `DESKTOP-123\John.Smith`).

- **Web resource address** – `%CANONIC_REQUEST_URL%`.

  Adresa zablokovaného webového prostředku.

- **Rule name** – `%RULE%`.

  Název pravidla, které zablokovalo webový prostředek.

- **Email for sending a message** – `%COMPLAIN_EMAIL%`.

  E-mailová adresa pro zpětnou vazbu k blokům webových prostředků. Kliknutím na e-mailovou adresu se otevře okno, ve kterém může uživatel napsat zprávu správci.

- **Name of content category** – `%CONTENT_CATEGORY_LIST%`.

  Kategorie webu, do které zablokovaný prostředek patří (například *Payment systems*).

- **Name of data type category** – `%TYPE_CATEGORY_LIST%`.

  Kategorie datového typu o zablokovaném webovém prostředku (například *Graphic files*).

- **Link to requested web resource** – `%CONTINUE_PAGE%`.

  Odkaz na požadovanou webovou stránku (např. `http://www.example.com/pagename.html`).

- **Link to website** – `%CONTINUE_SITE%`.

  Odkaz na webovou stránku, která obsahuje požadovanou webovou stránku (například `http://www.example.com/`).

- **Link for access to domains** – `%CONTINUE_DOMAIN%`.

  Odkaz, na který lze kliknout pro přístup na všechny stávající webové stránky s danou doménou. Pokud je například adresa zablokované webové stránky `http://www.example.com`, proměnná `%CONTINUE_DOMAIN%` je nahrazena odkazem `http://*.example.com`. Kliknutím na tento odkaz umožníte přístup ke všem webovým adresám názvu základní domény `http://www.example.com/` včetně subdomén, např. `http://start.example.com/*` nebo `http://domain.domain.example.com/*`, kde `*` znak je libovolná sekvence znaků (včetně prázdného řetězce).

Kontrola zařízení

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.

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 **Advanced** → **Repositories** → **Hardware**.

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 – ⊘.
  - Podle pravidel (pouze tiskárny a přenosná zařízení) – .
  - V závislosti na sběrnici připojení (kromě 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). Pokud je u typu zařízení vybrán režim **V závislosti na sběrnici připojení**, aplikace povolí nebo zakáže přístup k zařízení v závislosti na rozhraní připojení (např. 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.

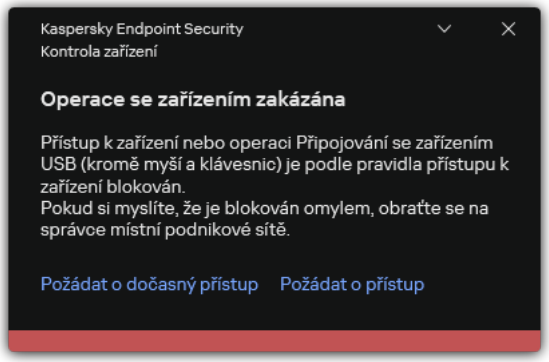
- **Zařízení dle masky ID**. Pokud používáte více zařízení s podobnými ID, můžete je přidat do seznamu důvěryhodných zařízení pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `WDC_C*`.

- **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.

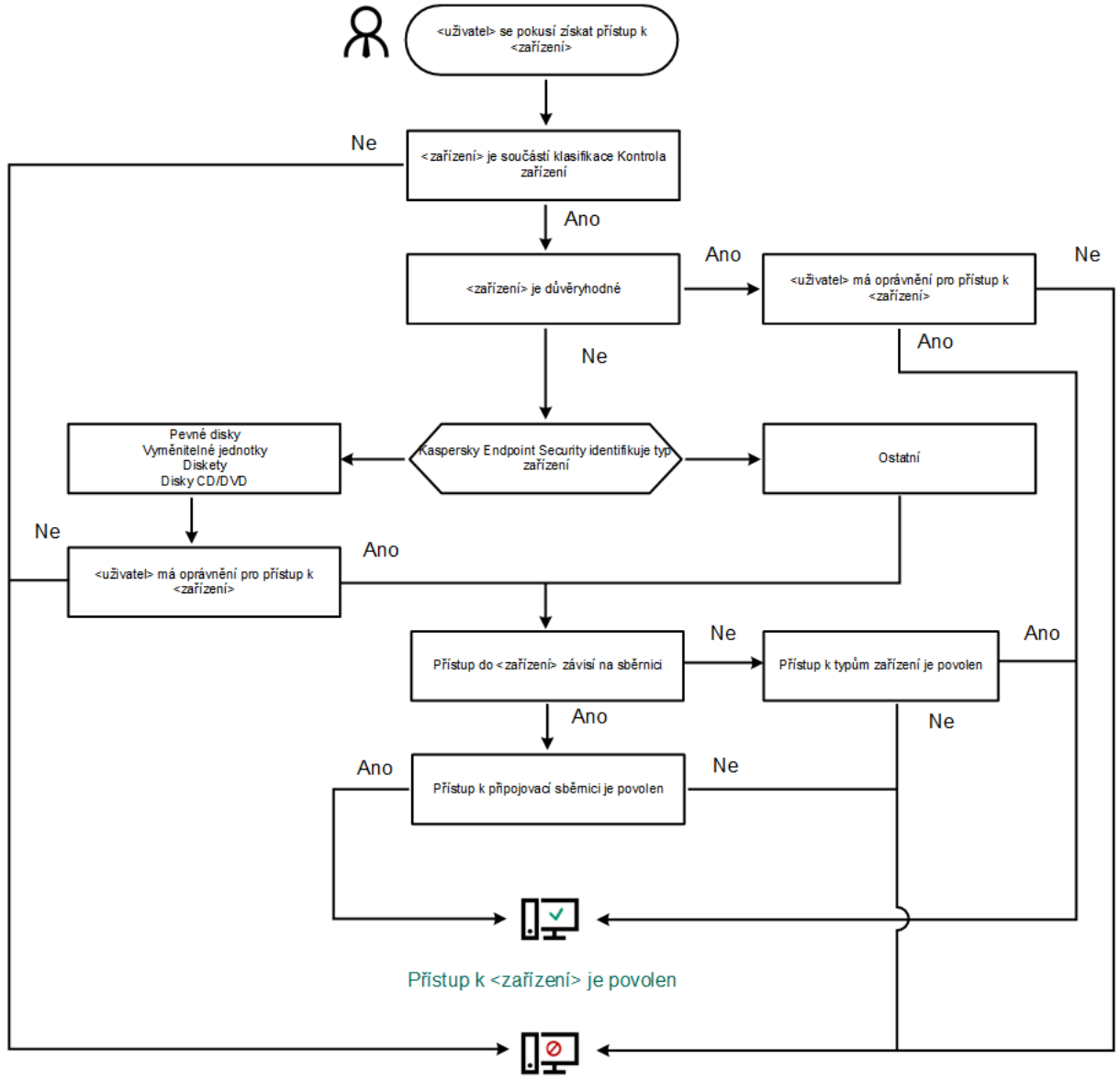
Když je k počítači připojeno zařízení, které je blokováno součástí Kontrola zařízení, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).



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.

O pravidlech přístupu

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. 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 (včetně USB flash disků).	✓	✓	✓	✓	✓

Diskety	✓	✓	✓	✓	✓
Disky CD/DVD	✓	✓	✓	✓	✓
Přenosná zařízení (MTP)	✓	✓	✓	✓	✓
Místní tiskárny	✓	–	✓	✓	–
Síťové tiskárny	✓	–	✓	✓	–
Modemy	✓	–	–	–	–
Pásková zařízení	✓	–	–	–	–
Multifunkční zařízení	✓	–	–	–	–
Čtečky karet	✓	–	–	–	–
Zařízení Windows CE USB ActiveSync	✓	–	–	–	–
Externí síťové adaptéry	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Fotoaparáty a skenery	✓	–	–	–	–

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 pro přístup ke sběrnici připojení

Pokud je u pravidla přístupu podle typu zařízení vybrána hodnota **V závislosti na sběrnici připojení**, aplikace povolí nebo zakáže přístup k zařízení v závislosti na rozhraní připojení. Pravidla povolující přístup ke sběrnicím jsou ve výchozím nastavení vytvořena pro všechny sběrnice připojení přítomné v rámci klasifikace součásti Kontrola zařízení.

Pravidla přístupu ke sběrnici připojení určují, zda je povoleno (stav ✓) nebo zakázáno (stav ⊘) připojení zařízení. Priorita pravidel přístupu podle typu zařízení je vyšší než priorita pravidel pro přístup ke sběrnici připojení.

Klávesnici a myš nelze pomocí součásti Kontrola zařízení uzamknout. Pokud zakážete přístup ke sběrnici USB, bude uživatel nadále pracovat s klávesnicí a myší připojenou přes USB. Součást Ochrana před útoky BadUSB má bránit tomu, aby se infikovaná zařízení USB napodobující klávesnici připojila k počítači.

Správa přístupu k zařízením podle typu

Kontrola zařízení umožňuje spravovat přístup k zařízením podle typu. Typ zařízení je určen operačním systémem v době připojení zařízení. Typ zařízení můžete vyhledat pomocí nástroje Správce zařízení, který je součástí operačního systému. Chcete-li spravovat přístup k zařízením, musíte nakonfigurovat pravidla. *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. Nemůžete přidat zařízení, které je mimo klasifikaci součásti Kontrola zařízení. Přístup k takovým zařízením je povolen všem uživatelům.

Součást Kontrola zařízení ve výchozím nastavení umožňuje přístup ke všem zařízením pro všechny uživatele.

Přístup k zařízením můžete nakonfigurovat následujícím způsobem:

- **Povolit**.

  Aplikace Kaspersky Endpoint Security uděluje všem uživatelům plný přístup k zařízení.

- **Blokovat**.

  Aplikace Kaspersky Endpoint Security blokuje připojení zařízení. Aplikace umožňuje připojení pouze k důvěryhodným zařízením.

- **V závislosti na sběrnici připojení**.

  Aplikace Kaspersky Endpoint Security určuje rozhraní připojení zařízení a omezuje přístup k zařízením na základě jejich stavu připojení ke sběrnici. Aplikace také umožňuje připojování důvěryhodných zařízení.

- **Podle pravidel**.

  U některých typů zařízení můžete určit jednotlivé uživatele nebo skupinu uživatelů, kteří smějí zařízení používat, nastavit plán přístupu k zařízením a nakonfigurovat oprávnění pro čtení a zápis. Aplikace také umožňuje připojování důvěryhodných zařízení.

Buďte opatrní při konfiguraci přístupu k zařízením typu **Pevné disky**. Pokud zablokujete přístup na systémový disk, aplikace může způsobit selhání (BSOD) při spouštění operačního systému.

Pokud zařízení neodpovídá klasifikačnímu schématu součásti Kontrola zařízení, přístup k takovému zařízení nelze omezit.

Jak spravovat přístup k zařízením podle typu v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
5. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.
   Na kartě **Typy zařízení** se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.
6. Postup konnfigurace pravidel přístupu pro zařízení:
   a. Vyberte režim přístupu: **Povolit**, **Blokovat**, **V závislosti na sběrnici připojení**, **Podle pravidel**.
      Chcete-li vybrat režim **Podle pravidel**, musíte dvojitým kliknutím otevřít vlastnosti pravidla přístupu.
   b. Pokud vyberete režim přístupu **V závislosti na sběrnici připojení**, musíte nakonfigurovat pravidla přístupu pro rozhraní připojení na kartě **Sběrnice připojení**.
   c. V případě úložných zařízení (například vyměnitelných médií) můžete nakonfigurovat přístupová oprávnění pro jednotlivé uživatele. Můžete také nastavit plán přístupu k zařízením a nakonfigurovat oprávnění pro čtení a zápis.
      Tato zařízení můžete přidat na seznam důvěryhodných zařízení. *Důvěryhodná zařízení* jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.
   d. V případě potřeby nakonfigurujte pravidla tisku.
   e. V případě potřeby nakonfigurujte pravidla přístupu k zařízením Bluetooth.
   f. V případě potřeby nakonfigurujte pravidla připojení k počítačům s Wi-Fi.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak spravovat přístup k zařízením podle typu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Device Control**.
5. V části **Device access rules** vyberte kartu **Devices and Wi-Fi networks**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
6. Postup konnfigurace pravidel přístupu pro zařízení:
   a. Vyberte režim přístupu: **Allow**, **Block**, **Depends on bus**, **Custom**.
      Pokud v rozevírací nabídce režim přístupu chybí, otevřete vlastnosti pravidla přístupu dvojitým kliknutím na typ zařízení.
   b. Pokud vyberete režim přístupu **Depends on bus**, musíte nakonfigurovat pravidla přístupu pro rozhraní připojení na kartě **Connection buses**.
   c. V případě úložných zařízení (například vyměnitelných médií) můžete nakonfigurovat přístupová oprávnění pro jednotlivé uživatele. Můžete také nastavit plán přístupu k zařízením a nakonfigurovat oprávnění pro čtení a zápis.
      Tato zařízení můžete přidat na seznam důvěryhodných zařízení. *Důvěryhodná zařízení* jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

d. V případě potřeby nakonfigurujte pravidla tisku.

e. V případě potřeby nakonfigurujte pravidla přístupu k zařízením Bluetooth.

f. V případě potřeby nakonfigurujte pravidla připojení k počítačům s Wi-Fi.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak spravovat přístup k zařízením v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** klikněte na odkaz **Zařízení a Wi-Fi sítě**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
4. Postup konnfigurace pravidel přístupu pro zařízení:
   a. Vyberte režim přístupu: **Povolit**, **Blokovat**, **V závislosti na sběrnici připojení**, **Podle pravidel**.
      Pokud v rozevírací nabídce režim přístupu chybí, otevřete vlastnosti pravidla přístupu dvojitým kliknutím na typ zařízení.
   b. Pokud vyberete režim přístupu **V závislosti na sběrnici připojení**, musíte nakonfigurovat pravidla přístupu pro rozhraní připojení na kartě **Sběrnice připojení**.
   c. V případě úložných zařízení (například vyměnitelných médií) můžete nakonfigurovat přístupová oprávnění pro jednotlivé uživatele. Můžete také nastavit plán přístupu k zařízením a nakonfigurovat oprávnění pro čtení a zápis.
      Tato zařízení můžete přidat na seznam důvěryhodných zařízení. *Důvěryhodná zařízení* jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.
   d. V případě potřeby nakonfigurujte pravidla tisku.
   e. V případě potřeby nakonfigurujte pravidla přístupu k zařízením Bluetooth.
   f. V případě potřeby nakonfigurujte pravidla připojení k počítačům s Wi-Fi.
5. Uložte změny.

Když se tak uživatel pokusí získat přístup k zařízení, aplikace zablokuje přístup v souladu s pravidly. Aplikace Kaspersky Endpoint Security také příslušnou událost zaprotokoluje. Pokud chcete přístup udělit jednotlivým zařízením, můžete přidat tato zařízení na seznam důvěryhodných zařízení.

Správa přístupu k zařízením pomocí připojovací sběrnice

Postup úpravy pravidla přístupu ke sběrnici připojení:

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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 **Blokovat**.

   Pokud jste změnili přístup ke sběrnici připojení **Sériový port** (COM) nebo **Paralelní port** (LPT), musíte pro aktivaci pravidla přístupu restartovat počítač.

6. Uložte změny.

Rozlišení přístupových práv uživatelů k zařízením

Přístupová práva uživatele můžete nakonfigurovat podle typu zařízení nebo k důvěryhodným zařízením.

Rozlišení přístupových práv uživatelů podle typu zařízení

Kontrola zařízení umožňuje konfiguraci přístupových práv uživatelů k datům na *paměťových zařízeních*. U takovýchto zařízení můžete nakonfigurovat oprávnění k zápisu a čtení. Kontrola zařízení podporuje následující typy *paměťových zařízení*:

- Pevné disky
- Vyměnitelné jednotky (včetně USB flash disků)
- Diskety
- Disky CD/DVD
- Přenosná zařízení (MTP) Mezi přenosná zařízení (MTP) patří například mobilní zařízení, fotoaparáty, přehrávače médií a tak dále.

Tímto způsobem můžete například povolit používání vyměnitelných médií pouze skupině správců. U jiných typů zařízení můžete zakázat nebo povolit přístup všem uživatelům. Také můžete nakonfigurovat přístupová práva uživatelů pro používání tiskáren.

Jak nakonfigurovat přístupová práva uživatele k datům na úložných zařízeních v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
5. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.
   Na kartě **Typy zařízení** se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.
6. Chcete-li nakonfigurovat pravidla přístupu k úložným zařízením, dvojitým kliknutím otevřete seznam pravidel.
7. Postup konfigurace pravidla přístupu k mobilním zařízení:
   a. V bloku **Pravidla přístupu** klikněte na tlačítko **Přidat**.
      Otevře se okno pro přidání nového pravidla přístupu k úložnému zařízení.
   b. V poli **Priorita pravidla** nastavte prioritu *zápisu pravidla*. 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.
   c. V části **Pravidlo pro uživatele a skupiny** vyberte uživatele nebo skupiny uživatelů. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
   d. Klikněte na tlačítko **OK**.
8. V části **Plány pro vybrané pravidlo přístupu** nakonfigurujte plán přístupu k úložnému zařízení pro uživatele.
   Můžete například uživatelům povolit používání úložných zařízení pouze během pracovní doby.
9. Nakonfigurujte přístupová oprávnění uživatelů k úložným zařízením ve správci souborů (**Čtení** / **Zápis**).
10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak nakonfigurovat přístupová práva uživatele k datům na úložných zařízeních ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls → Device Control**.

5. V bloku **Device access rules** na kartě pravidel přístupu otevřete vlastnosti pravidla přístupu pro úložná zařízení.

6. V bloku **Device access rules** vyberte položku **Custom**.

7. Postup konfigurace pravidla přístupu k mobilním zařízení:

   a. V bloku **Users and their rights** klikněte na tlačítko **Add**.

      Otevře se okno pro přidání nového pravidla přístupu k úložnému zařízení.

   b. V poli **Priority** nastavte prioritu *zápisu pravidla*. 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.

   c. V části **User or group** vyberte uživatele nebo skupiny uživatelů. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   d. V části **Access schedule** nakonfigurujte plán přístupu k úložnému zařízení pro uživatele.

      Můžete například uživatelům povolit používání úložných zařízení pouze během pracovní doby.

   e. Nakonfigurujte přístupová oprávnění uživatelů k úložným zařízením ve správci souborů (**Read** / **Write**).

   f. Klikněte na tlačítko **Save**.

8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak nakonfigurovat přístupová práva uživatele k datům na úložných zařízeních v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola zařízení**.

3. V bloku **Nastavení přístupu** klikněte na odkaz **Zařízení a Wi-Fi sítě**.

   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.

4. Chcete-li nakonfigurovat pravidla přístupu k mobilním zařízením, kliknutím pravým tlačítkem otevřete seznam pravidel.

5. Postup konfigurace pravidla přístupu k mobilním zařízení:

   a. V bloku **Oprávnění uživatele** klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla přístupu k úložnému zařízení.

   b. V poli **Priorita** nastavte prioritu *zápisu pravidla*. 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.

   c. V části **Uživatelé** vyberte uživatele nebo skupiny uživatelů. Můžete vybrat uživatele ve službě Active Directory nebo ručně zadat místní uživatelské jméno. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   d. Klikněte na tlačítko **OK**.

6. V části **Plánování přístupu k zařízením** nakonfigurujte plán přístupu k úložnému zařízení pro uživatele.

   Můžete například uživatelům povolit používání úložných zařízení pouze během pracovní doby.

7. Nakonfigurujte přístupová oprávnění uživatelů k úložným zařízením ve správci souborů (**Čtení** / **Zápis**).

8. Uložte změny.

Rozlišení přístupových práv uživatelů k důvěryhodným zařízením

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. Můžete nakonfigurovat přístupová práva uživatele ve vlastnostech důvěryhodného zařízení.

Správa přístupu k mobilním zařízením

Kaspersky Endpoint Security vám umožňuje řídit přístup k datům na mobilních zařízeních se systémem Android a iOS. Mobilní zařízení patří do kategorie přenosných zařízení (MTP). Chcete-li tedy nakonfigurovat přístup k datům na mobilních zařízeních, musíte upravit nastavení přístupu pro 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 a zvoleném režimu připojení USB. Kaspersky Endpoint Security umožňuje konfigurovat individuální přístupová oprávnění pro data na mobilních zařízeních v aplikacích ADB, iTunes nebo správci souborů. Ve všech ostatních případech umožňuje součást Kontrola zařízení přístup k mobilním zařízením v souladu s pravidly pro přístup k přenosným zařízením (MTP).

Přístup k mobilním zařízením

Mobilní zařízení patří do kategorie přenosných zařízení (MTP), proto je jejich nastavení stejné. Můžete vybrat jeden z následujících režimů přístupu k mobilním zařízením:

- **Povolit** ✓. Aplikace Kaspersky Endpoint Security umožňuje plný přístup k mobilním zařízením. Soubory můžete otevírat, vytvářet, upravovat, kopírovat nebo odstraňovat na mobilních zařízeních pomocí správce souborů nebo aplikací ADB a iTunes. Baterii zařízení můžete také nabíjet připojením mobilního zařízení k portu USB počítače.

- **Blokovat** ⊘. Aplikace Kaspersky Endpoint Security omezuje přístup k mobilním zařízením ve správci souborů a aplikacím ADB a iTunes. Aplikace umožňuje přístup pouze k důvěryhodným mobilním zařízením. Baterii zařízení můžete také nabíjet připojením mobilního zařízení k portu USB počítače.

- **V závislosti na sběrnici připojení**. Aplikace Kaspersky Endpoint Security umožňuje připojení k mobilním zařízení v souladu se stavem připojení USB (**Povolit** ✓ nebo **Blokovat** ⊘).

- **Podle pravidel**. Aplikace Kaspersky Endpoint Security omezuje přístup k mobilním zařízením v souladu s pravidly. V pravidlech můžete nakonfigurovat přístupová práva (čtení/zápis), vybrat uživatele nebo skupinu uživatelů, kteří mohou mít přístup k mobilním zařízením (MTP), a nakonfigurovat plán přístupu pro mobilní zařízení. Přístup k datům na mobilních zařízeních můžete také omezit pomocí aplikace ADB a iTunes.

Konfigurace pravidel přístupu k mobilním zařízením

Pravidla přístupu pro přenosná zařízení (MTP), zařízení ADB a zařízení iTunes jsou nakonfigurována odlišně. Pro přenosná zařízení (MTP) a zařízení ADB můžete nakonfigurovat pravidla pro jednotlivé uživatele nebo skupiny uživatelů a vytvořit plán, kdy budou pravidla platit. U zařízení iTunes to nemůžete udělat. Všem uživatelům můžete povolit nebo zakázat přístup k datům pouze prostřednictvím aplikace iTunes.

Jak konfigurovat pravidla přístupu k mobilním zařízením v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.

4. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.

   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.

5. V místní nabídce u typu zařízení **Přenosná zařízení (MTP)** nakonfigurujte režim přístupu k mobilnímu zařízení: **Povolit** ✓, **Blokovat** ⊘ nebo **V závislosti na sběrnici připojení**.

6. Chcete-li nakonfigurovat pravidla přístupu k mobilním zařízením, dvojitým kliknutím otevřete seznam pravidel.

7. Nakonfigurujte pravidlo přístupu k mobilnímu zařízení:

   a. V bloku **Pravidla přístupu** klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla přístupu k mobilnímu zařízení.

b. V poli **Priorita** nastavte prioritu zápisu pravidla. Pravidlo obsahuje následující atributy: uživatelský účet, plán, oprávnění (čtení / zápis / přístup ADB) 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.

c. V části **Pravidlo pro uživatele a skupiny** vyberte uživatele nebo skupiny uživatelů. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

d. Klikněte na tlačítko **OK**.

8. V části **Plány pro vybrané pravidlo přístupu** nakonfigurujte plán přístupu k zařízení pro uživatele.

Konfigurace samostatného plánu přístupu pro zařízení ADB není možná. Můžete nakonfigurovat společný plán přístupu pro zařízení ADB a přenosná zařízení (MTP).

9. Nakonfigurujte přístupová oprávnění uživatelů k mobilním zařízením ve správci souborů (**Čtení** / **Zápis**).

10. Přístup k datům na mobilním zařízení můžete nakonfigurovat prostřednictvím aplikace ADB pomocí zaškrtávacího políčka **Přístup prostřednictvím ADB**.

Pokud políčko není zaškrtnuto, je při připojení mobilního zařízení zabráněno aplikaci ADB detekovat zařízení.

11. V části **Přístup prostřednictvím iTunes** nakonfigurujte přístup k datům na mobilním zařízení prostřednictvím aplikace iTunes.

Kaspersky Endpoint Security použije nastavení pro přístup k mobilnímu zařízení prostřednictvím aplikace iTunes pro všechny uživatele. Konfigurace samostatného plánu přístupu pro zařízení iTunes není možná.

12. Uložte změny.

Jak konfigurovat pravidla přístupu k mobilním zařízením ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls** → **Device Control**.

5. V bloku **Device access rules** klikněte na odkaz **Devices and Wi-Fi networks**.

V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.

6. Vyberte typ zařízení **Portable devices (MTP)**.

Otevřou se přístupová práva k přenosným zařízením (MTP).

7. Nakonfigurujte režim přístupu k mobilním zařízením: **Allow**, **Block**, **Depends on bus** nebo **Custom**.

8. Pomocí přepínače **Access via iTunes for all users ENABLED** nakonfigurujte přístup k datům na mobilním zařízení prostřednictvím aplikace iTunes.

Kaspersky Endpoint Security použije nastavení pro přístup k mobilnímu zařízení prostřednictvím aplikace iTunes pro všechny uživatele. Konfigurace samostatného plánu přístupu pro zařízení iTunes není možná.

9. Pokud vyberete možnost **Custom**, musíte přidat pravidla přístupu pro zařízení. Chcete-li tak učinit, v části **Users and their rights** klikněte na tlačítko **Add** a nakonfigurujte pravidlo přístupu k mobilnímu zařízení:

a. V poli **Priority** nastavte prioritu zápisu pravidla. Pravidlo obsahuje následující atributy: uživatelský účet, plán, oprávnění (čtení / zápis / přístup ADB) 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.

b. V části **User or group** vyberte uživatele nebo skupiny uživatelů pro přístup k mobilním zařízením. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

c. V části **Access schedule** nakonfigurujte plán přístupu k zařízení pro uživatele.

> Konfigurace samostatného plánu přístupu pro zařízení ADB není možná. Můžete nakonfigurovat společný plán přístupu pro zařízení ADB a přenosná zařízení (MTP).

d. Nakonfigurujte přístupová oprávnění uživatelů k mobilním zařízením ve správci souborů (**Read** / **Write**).

e. Přístup k datům na mobilním zařízení můžete nakonfigurovat prostřednictvím aplikace ADB pomocí zaškrtávacího políčka **Access via ADB**.

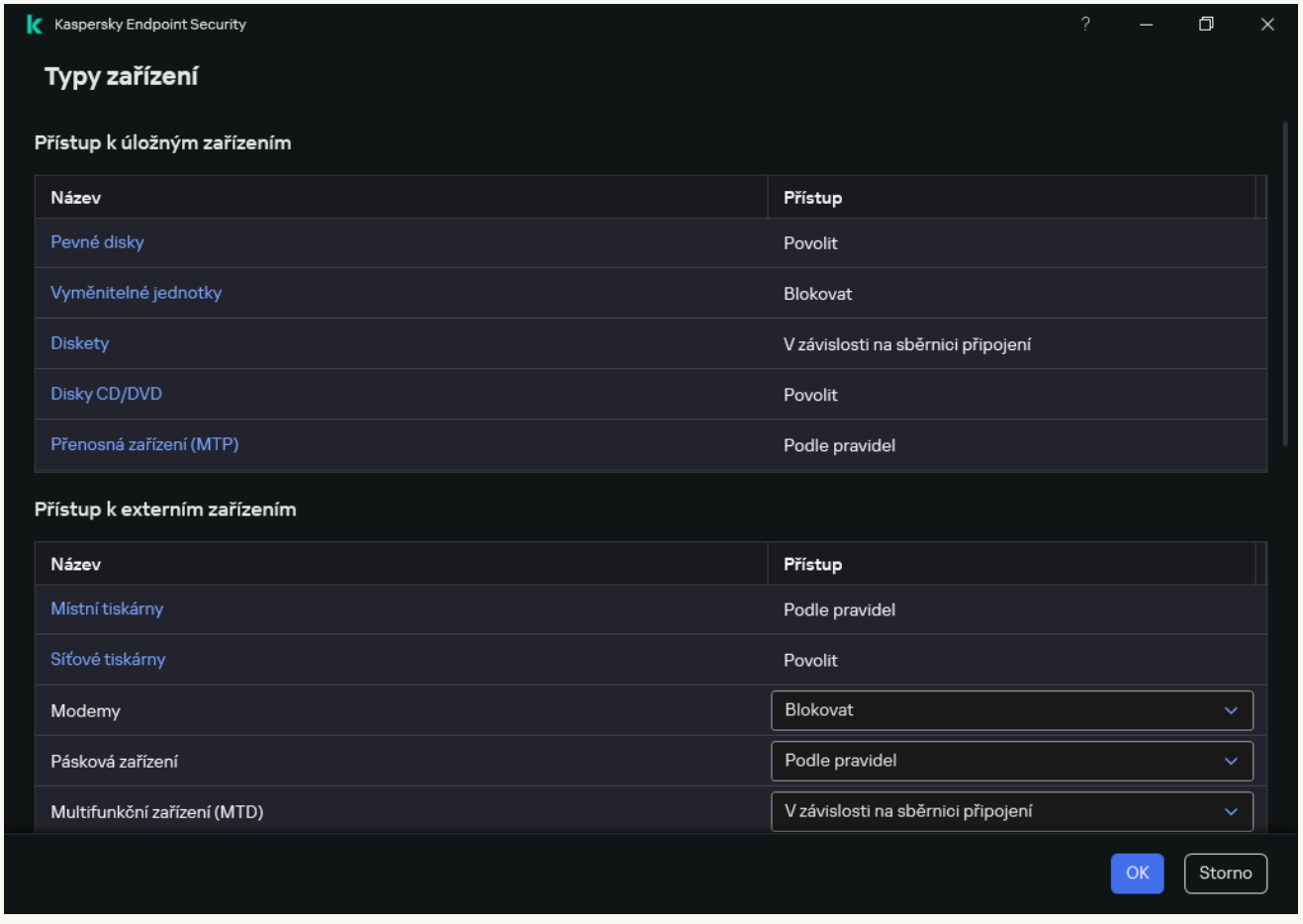
Pokud políčko není zaškrtnuto, je při připojení mobilního zařízení zabráněno aplikaci ADB detekovat zařízení.

10. Uložte změny.

Jak konfigurovat pravidla přístupu k mobilním zařízením v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení 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.



Typy zařízení v součásti Kontrola zařízení

4. V bloku **Přístup k úložným zařízením** klikněte na odkaz **Přenosná zařízení (MTP)**.

   Otevře se okno obsahující pravidla přístupu k přenosným zařízením (MTP).

5. V části **Přístup** nakonfigurujte režim přístupu k mobilním zařízením: **Povolit**, **Blokovat**, **V závislosti na sběrnici připojení** nebo **Podle pravidel**.

6. Pokud vyberete možnost **Podle pravidel**, musíte přidat pravidla přístupu pro zařízení:

   a. V bloku **Oprávnění uživatele** klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla přístupu k mobilnímu zařízení.

   b. V poli **Priorita** nastavte prioritu zápisu pravidla. Pravidlo obsahuje následující atributy: uživatelský účet, plán, oprávnění (čtení / zápis / přístup ADB) 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.

   c. V části **Stav** zapněte pravidlo přístupu k mobilním zařízením.

   d. V části **Pravidla přístupu** nakonfigurujte pro uživatele přístupová oprávnění k mobilním zařízením.

      - Nakonfigurujte přístupová oprávnění uživatelů k mobilním zařízením ve správci souborů (**Čtení** / **Zápis**).
      - Přístup k datům na mobilním zařízení můžete nakonfigurovat prostřednictvím aplikace ADB pomocí zaškrtávacího políčka **Přístup prostřednictvím ADB**.

        Pokud políčko není zaškrtnuto, je při připojení mobilního zařízení zabráněno aplikaci ADB detekovat zařízení.

   e. V části **Uživatelé** vyberte uživatele nebo skupiny uživatelů pro přístup k mobilním zařízením. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   f. V části **Plánování přístupu k zařízením** nakonfigurujte pro uživatele plán přístupu k zařízení.

      Konfigurace samostatného plánu přístupu pro zařízení ADB není možná. Můžete nakonfigurovat společný plán přístupu pro zařízení ADB a přenosná zařízení (MTP).

   g. V části **Přístup prostřednictvím iTunes** nakonfigurujte přístup k datům na mobilním zařízení prostřednictvím aplikace iTunes.

      Kaspersky Endpoint Security použije nastavení pro přístup k mobilnímu zařízení prostřednictvím aplikace iTunes pro všechny uživatele. Konfigurace samostatného plánu přístupu pro zařízení iTunes není možná.

7. Uložte změny.

Přístup uživatelů k mobilním zařízením je tak omezen v souladu s pravidly. Pokud jste zakázali přístup k mobilním zařízením v aplikacích ADB a iTunes, aplikace ADB a iTunes nemohou toto zařízení při připojení detekovat.

Důvěryhodná mobilní zařízení

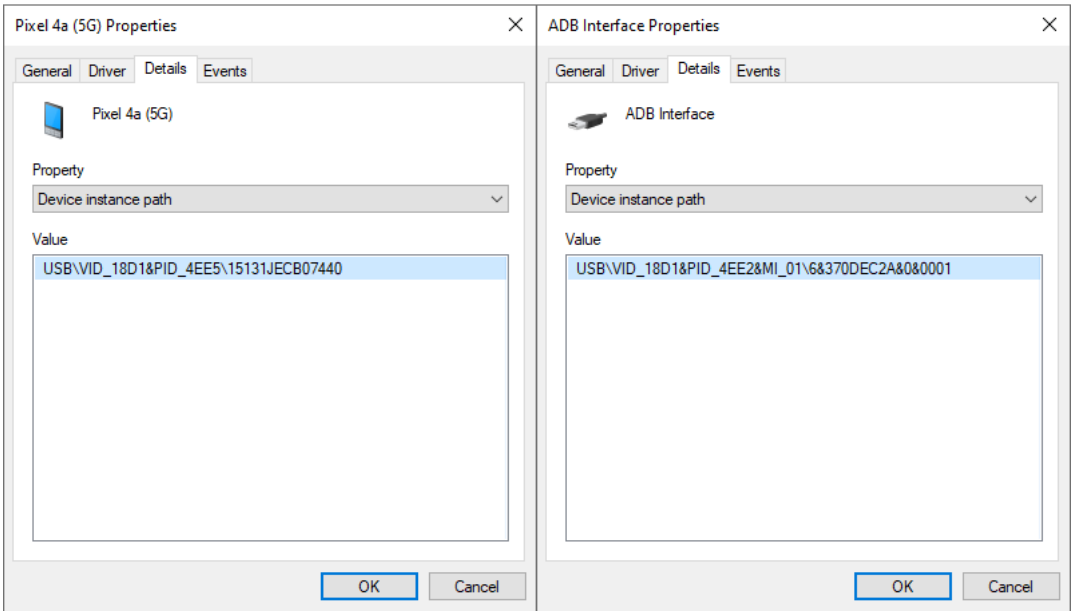
Důvěryhodná zařízení jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

Postup pro přidání důvěryhodného mobilního zařízení je úplně stejný jako u jiných typů důvěryhodných zařízení. Mobilní zařízení můžete přidat podle ID nebo modelu zařízení.

Chcete-li přidat důvěryhodné mobilní zařízení podle ID, budete potřebovat jedinečné ID (Hardware ID – HWID). ID najdete ve vlastnostech zařízení pomocí nástrojů operačního systému (viz obrázek níže). Umožňuje vám to nástroj Správce zařízení. ID přenosných zařízení (MTP) a zařízení ADB a iTunes se liší i u stejného mobilního zařízení. ID přenosného zařízení (MTP) může vypadat takto: `15131JECB07440`. ID zařízení ADB může vypadat takto: `6&370DEC2A&0&0001`. Přidání zařízení podle ID je praktické, když chcete přidat několik konkrétních zařízení. Můžete použít i masky.

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.

Chcete-li přidat důvěryhodné mobilní zařízení podle modelu zařízení, budete potřebovat její Vendor ID (VID) a Product ID (PID). ID najdete ve vlastnostech zařízení pomocí nástrojů operačního systému (viz obrázek níže). Šablona pro zadání VID a PID: `VID_18D1&PID_4EE5`. Přidání zařízení podle modelu je praktické, pokud v organizaci používáte zařízení určitého modelu. Tímto způsobem můžete přidat všechna zařízení tohoto modelu.



ID zařízení ve Správci zařízení

Správa přístupu k zařízením Bluetooth

Kaspersky Endpoint Security umožňuje spravovat přístup k zařízením Bluetooth. Mezi zařízení Bluetooth patří bezdrátové klávesnice, myši, náhlavní soupravy, tiskárny atd. Bluetooth můžete také používat pro komunikaci např. s mobilním zařízením.

Při připojení nebo odpojení zařízení Bluetooth může aplikace vytvořit o zařízení více událostí. Důvodem je, že operační systém může rozpoznat zařízení Bluetooth jako více zařízení různých typů. Kaspersky Endpoint Security také spravuje adaptér Bluetooth, přes který je zařízení připojeno jako samostatné zařízení. Aplikace proto vytvoří událost pro každé z detekovaných zařízení.

Můžete vybrat jeden z následujících režimů přístupu k zařízením Bluetooth:

- **Povolit a nezaznamenávat do protokolu** . Kaspersky Endpoint Security umožňuje připojení jakýchkoli zařízení Bluetooth a neukládá informace o připojení do protokolu událostí. Můžete připojit vstupní zařízení Bluetooth (klávesnice, myši atd.), odesílat data přes Bluetooth, spravovat další zařízení Bluetooth (náhlavní souprava, sluchátka atd.).
- **Povolit** . Kaspersky Endpoint Security umožňuje připojení jakýchkoli zařízení Bluetooth. Můžete připojit vstupní zařízení Bluetooth (klávesnice, myši atd.), odesílat data přes Bluetooth, spravovat další zařízení Bluetooth (náhlavní souprava, sluchátka atd.).
- **Blokovat** . Aplikace Kaspersky Endpoint Security omezuje přístup k zařízením Bluetooth. Můžete povolit připojení pouze vstupních zařízení Bluetooth (třída Human Interface Devices). Mezi tato zařízení patří klávesnice, zařízení s funkcí myši, joysticky atd.

Není možné vytvořit seznam důvěryhodných zařízení Bluetooth. Pokud máte omezený přístup k zařízením Bluetooth, můžete připojovat pouze vstupní zařízení Bluetooth.

Jak konfigurovat pravidla přístupu k zařízením Bluetooth v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
5. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
6. V místní nabídce u typu zařízení **Bluetooth** nakonfigurujte režim přístupu k zařízení Bluetooth: **Povolit** , **Blokovat** nebo **Povolit a nezaznamenávat do protokolu** .

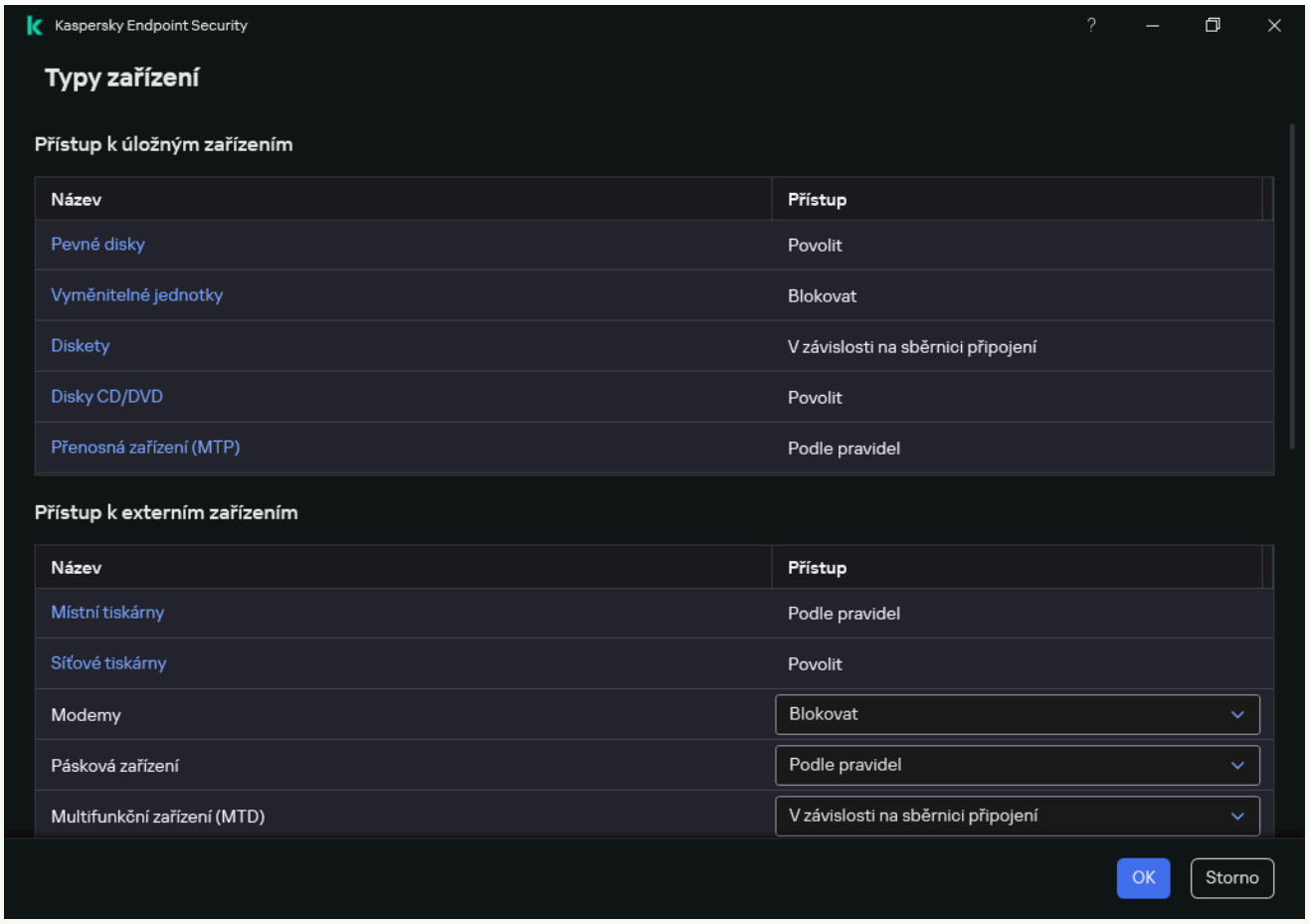
7. Pokud vyberete **Blokovat**, můžete povolit připojení pouze vstupních zařízení Bluetooth (klávesnice, myši atd.). To provedete tak, že v části **Výjimky** zaškrtnete políčko **Vstupní zařízení (myš a klávesnice)**.
8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak konfigurovat pravidla přístupu k zařízením Bluetooth ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Device Control**.
5. V bloku **Device access rules** klikněte na odkaz **Devices and Wi-Fi networks**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
6. Vyberte typ zařízení **Bluetooth devices**.
   Otevře se nastavení přístupu k zařízení Bluetooth.
7. Nakonfigurujte režim přístupu zařízení Bluetooth: **Allow**, **Block**, **Allow and do not log**.
8. Pokud vyberete **Block**, můžete povolit připojení pouze vstupních zařízení Bluetooth (klávesnice, myši atd.). To provedete tak, že v části **Exclusions** zaškrtnete políčko **Input devices (mice and keyboards)**.
9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak konfigurovat pravidla přístupu k zařízením Bluetooth v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení 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.



Typy zařízení v součásti Kontrola zařízení

4. V bloku **Přístup k externím zařízením** klikněte na odkaz **Bluetooth**.
   Otevře se nastavení přístupu k zařízení Bluetooth.
5. V části **Přístup** nakonfigurujte režim přístupu k zařízením Bluetooth: **Povolit**, **Blokovat**, **Povolit a nezaznamenávat do protokolu**.
6. Pokud vyberete **Blokovat**, můžete povolit připojení pouze vstupních zařízení Bluetooth (klávesnice, myši atd.). To provedete tak, že v části **Výjimky** zaškrtnete políčko **Vstupní zařízení (myš a klávesnice)**.
7. Uložte změny.

Ovládání tisku

Řízení tisku není podporováno na počítačích s architekturou ARM.

Ovládání tisku můžete použít ke konfiguraci přístupu uživatelů k místním a síťovým tiskárnám.

Ovládání místní tiskárny

Kaspersky Endpoint Security umožňuje konfiguraci přístupu k místním tiskárnám na dvou úrovních: *připojení* a *tisk*.

Kaspersky Endpoint Security řídí připojení místní tiskárny prostřednictvím následujících sběrnic: USB, sériový port (COM), paralelní port (LPT).

Kaspersky Endpoint Security řídí připojení místních tiskáren k portům COM a LPT pouze na úrovni sběrnice. Chcete-li tedy zabránit připojení tiskárny přes porty COM a LPT, musíte to udělat výběrem režimu přístupu V závislosti na sběrnici připojení pro místní tiskárny a zákazem připojení ke sběrnicím COM a LPT.

U tiskáren připojených k USB vykonává aplikace řízení na dvou úrovních: typ zařízení (místní tiskárny) a sběrnice připojení (USB).

Můžete vybrat jeden z následujících režimů přístupu k místním tiskárnám přes USB:

- **Povolit** ✓. Kaspersky Endpoint Security uděluje všem uživatelům úplný přístup k místním tiskárnám. Uživatelé se mohou připojovat k tiskárnám a tisknout dokumenty pomocí prostředků, které poskytuje operační systém.

- **Blokovat**. Kaspersky Endpoint Security blokuje připojení k místním tiskárnám. Aplikace umožňuje pouze připojení k důvěryhodným tiskárnám.
- **V závislosti na sběrnici připojení**. Kaspersky Endpoint Security umožňuje připojení k místním tiskárnám v souladu se USB stavem sběrnice připojení (**Povolit** nebo **Blokovat**).
- **Podle pravidel**. Chcete-li ovládat tisk, musíte přidat *pravidla tisku*. V pravidlech můžete vybrat uživatele nebo skupinu uživatelů, kterým chcete povolit nebo zablokovat přístup k tisku dokumentů na lokálních tiskárnách.

Ovládání síťové tiskárny

Kaspersky Endpoint Security umožňuje konfiguraci přístupu k tisku na síťových tiskárnách. Můžete vybrat jeden z následujících režimů přístupu k síťovým tiskárnám:

- **Povolit a nezaznamenávat do protokolu**. Kaspersky Endpoint Security neřídí tisk na síťových tiskárnách. Aplikace uděluje přístup k tisku všem uživatelům a neukládá informace o tisku do protokolu událostí.
- **Povolit**. Kaspersky Endpoint Security udělují přístup k tisku na síťových tiskárnách všem uživatelům.
- **Blokovat**. Kaspersky Endpoint Security omezí přístup k síťovým tiskárnám všem uživatelům. Aplikace umožní přístup pouze k důvěryhodným tiskárnám.
- **Podle pravidel**. Kaspersky Endpoint Security uděluje přístup k tisku v souladu s pravidly tisku. V pravidlech můžete vybrat uživatele nebo skupinu uživatelů, kterým bude povolen nebo zakázán tisk dokumentů na síťové tiskárně.

Přidání pravidel tisku pro tiskárny

Jak přidat pravidla tisku v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
4. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.

   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
5. V místní nabídce pro typy zařízení **Místní tiskárny** a **Síťové tiskárny** nakonfigurujte režim přístupu pro příslušné tiskárny: **Povolit**, **Blokovat**, **Povolit a nezaznamenávat do protokolu** (pouze pro síťové tiskárny) nebo **V závislosti na sběrnici připojení** (pouze pro místní tiskárny).
6. Chcete-li konfigurovat pravidla tisku na místních a síťových tiskárnách, dvojitým kliknutím na seznamy pravidel tyto seznamy otevřete.
7. Jako režim přístupu k tiskárně vyberte **Podle pravidel**.
8. Vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo tisku.
   a. Klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla tisku.

   b. Přiřaďte položce pravidla prioritu. Záznam pravidla obsahuje následující atributy: uživatelský účet, akci (povolit/blokovat) a prioritu.

      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.

   c. V části **Akce** nakonfigurujte přístup uživatele k tisku na tiskárně.

   d. V části **Uživatelé a skupiny** vyberte uživatele nebo skupiny uživatelů pro přístup k tisku. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   e. Klikněte na tlačítko **OK**.
9. Uložte změny.

Jak přidat pravidlo tisku ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Device Control**.
5. V bloku **Device access rules** klikněte na odkaz **Devices and Wi-Fi networks**.

   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
6. Vyberte typ zařízení **Local printers** nebo **Network printers**.

   Otevřou se pravidla přístupu k tiskárně.
7. Nakonfigurujte režim přístupu pro příslušné tiskárny: **Allow**, **Block**, **Allow and do not log** (pouze pro síťové tiskárny), **Depends on bus** (pouze pro místní tiskárny) nebo **Custom**.
8. Pokud vyberete možnost **Custom**, musíte přidat pravidla tisku pro místní nebo síťové tiskárny. To provedete tak, že v tabulce s pravidly tisku kliknete na tlačítko **Add**.

   Otevře se nastavení nového pravidla tisku.
9. Přiřaďte položce pravidla prioritu. Záznam pravidla obsahuje následující atributy: uživatelský účet, akci (povolit/blokovat) a prioritu.

   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.

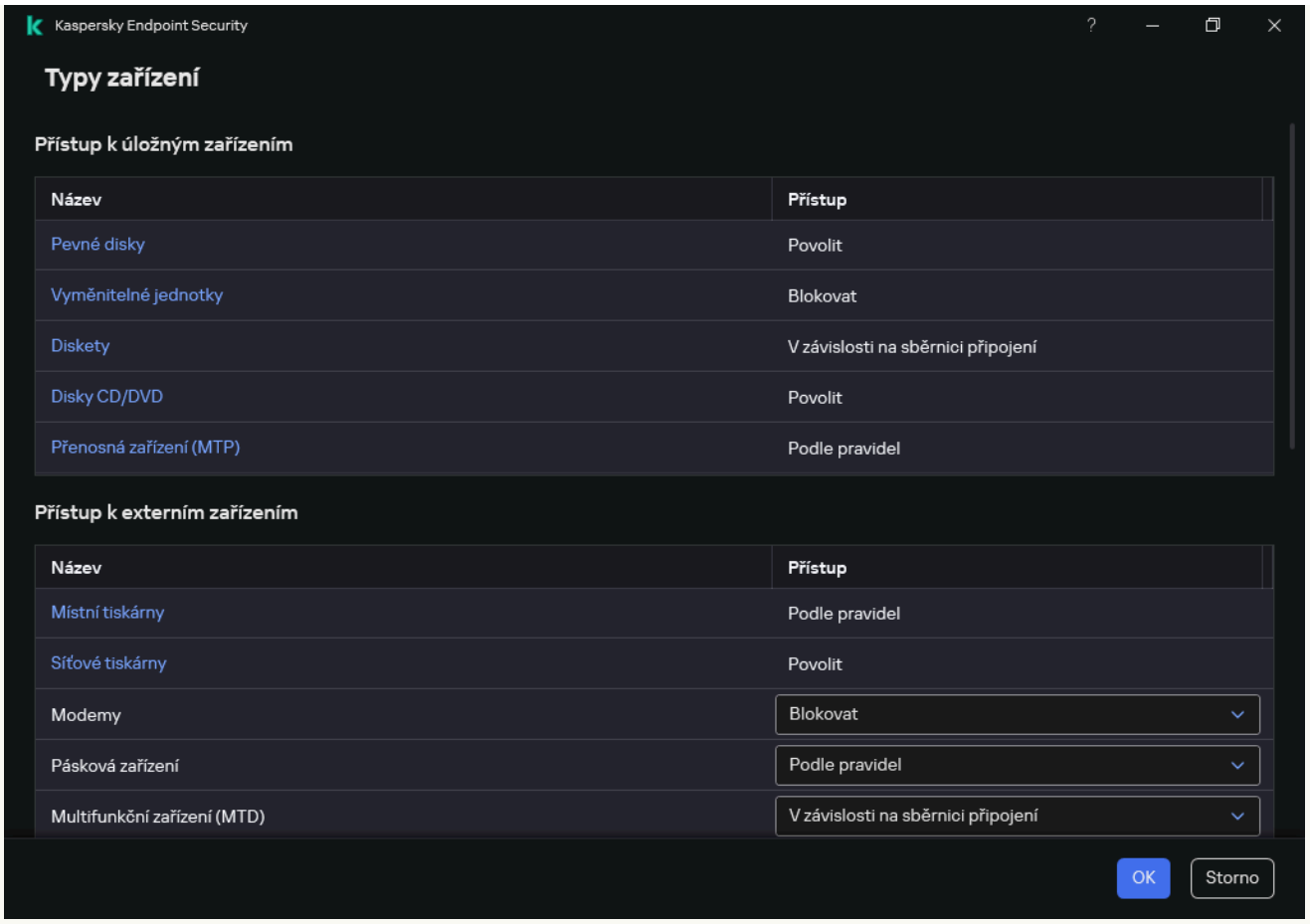
   Například můžete skupině Všichni udělit oprávnění jen pro čtení a skupině správců udělit oprávnění ke čtení a zápisu. Chcete-li tak učinit, přiřaďte skupině správců prioritu 1 a skupině Všichni prioritu 0.

   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.
10. V části **Action** nakonfigurujte přístup uživatele k tisku na tiskárně.
11. V části **User or group** vyberte uživatele nebo skupiny uživatelů pro přístup k tisku. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
12. Uložte změny.

Jak přidat pravidla tisku v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení 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.



Typy zařízení v součásti Kontrola zařízení

4. V části **Přístup k externím zařízením** klikněte na možnost **Místní tiskárny** nebo **Síťové tiskárny**.

   Otevře se okno s pravidly přístupu k tiskárně.

5. V části **Přístup k místním tiskárnám** nebo **Přístup k síťovým tiskárnám** nakonfigurujte režim přístupu pro tiskárny: **Povolit**, **Blokovat**, **Povolit a nezaznamenávat do protokolu** (pouze pro síťové tiskárny), **V závislosti na sběrnici připojení** (pouze pro místní tiskárny) nebo **Podle pravidel**.

6. Pokud vyberete možnost **Podle pravidel**, musíte přidat pravidla tisku pro tiskárny. Vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo tisku.

   a. Klikněte na tlačítko **Přidat**.

      Otevře se okno pro přidání nového pravidla tisku.

   b. Přiřaďte položce pravidla prioritu. Záznam pravidla obsahuje následující atributy: uživatelský účet, oprávnění (povolit/blokovat) a prioritu.

      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.

   c. V části **Akce** nakonfigurujte uživatelská oprávnění pro přístup k tisku.

   d. V části **Uživatelé a skupiny** vyberte uživatele nebo skupiny uživatelů pro přístup k tisku. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

7. Uložte změny.

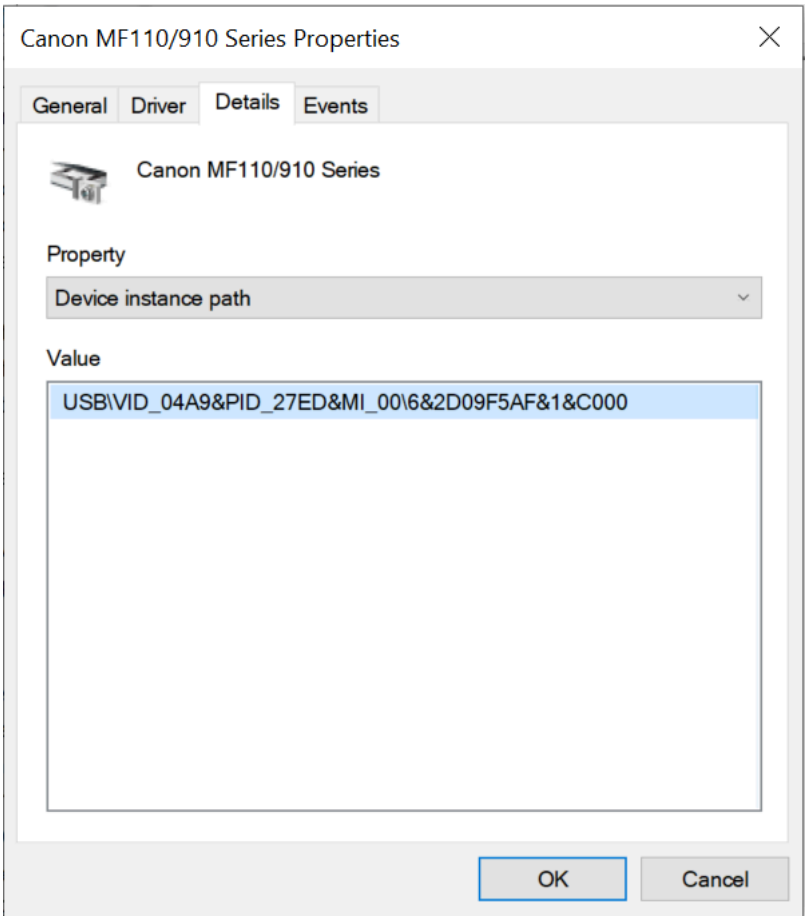
Důvěryhodné tiskárny

Důvěryhodná zařízení jsou zařízení, ke kterým mají uživatelé zadaní v nastavení důvěryhodných zařízeních neustálý a úplný přístup.

Postup pro přidání důvěryhodných tiskáren je úplně stejný jako u jiných typů důvěryhodných zařízení. Místní tiskárny můžete přidat podle ID nebo modelu zařízení. Síťové tiskárny můžete přidat pouze podle ID zařízení.

Chcete-li přidat důvěryhodnou místní tiskárnu podle ID, budete potřebovat jedinečné ID (Hardware ID – HWID). ID najdete ve vlastnostech zařízení pomocí nástrojů operačního systému (viz obrázek níže). Umožňuje vám to nástroj Device Manager. ID místní tiskárny může vypadat takto: `6&2D09F5AF&1&C000`. Přidání zařízení podle ID je praktické, když chcete přidat několik konkrétních zařízení. Můžete použít i masky.

Chcete-li přidat důvěryhodnou místní tiskárnu podle modelu zařízení, budete potřebovat její Vendor ID (VID) a Product ID (PID). ID najdete ve vlastnostech zařízení pomocí nástrojů operačního systému (viz obrázek níže). Šablona pro zadání VID a PID: `VID_04A9&PID_27FD`. Přidání zařízení podle modelu je praktické, pokud v organizaci používáte zařízení určitého modelu. Tímto způsobem můžete přidat všechna zařízení tohoto modelu.



ID zařízení ve Správci zařízení

Chcete-li přidat důvěryhodnou síťovou tiskárnu, budete potřebovat její ID zařízení. U síťových tiskáren může být ID zařízení síťový název tiskárny (název sdílené tiskárny), IP adresa tiskárny nebo adresa URL tiskárny.

Ovládání připojení k Wi-Fi

Součást Kontrola zařízení umožňuje spravovat připojení počítače (notebooku) k Wi-Fi. Veřejné Wi-Fi sítě mohou být nezabezpečené a používání takovýchto sítí může vést ke ztrátě dat. Součást Kontrola zařízení umožňuje zablokovat uživateli připojení k Wi-Fi nebo povolit připojení pouze k důvěryhodným sítím. Můžete například povolit připojení pouze k podnikové Wi-Fi síti, která je dostatečně zabezpečená. Kontrola zařízení bude blokovat přístup ke všem sítím Wi-Fi s výjimkou těch určených v seznamu důvěryhodných.

Pokud chcete na počítačích se systémem Windows 11 řídit připojení Wi-Fi, musíte povolit zjišťování polohy. Chcete-li to provést, musíte v nastavení operačního systému povolit přepínač **Zjišťování polohy** (**Nastavení** → **Soukromí a zabezpečení** → **Poloha**). Pokud je zjišťování polohy zakázáno, aplikace Kaspersky Endpoint Security neřídí připojení k sítím Wi-Fi.

Jak omezit připojení k Wi-Fi v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
4. V části **Nastavení součásti Kontrola zařízení** vyberte kartu **Typy zařízení**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
5. V místní nabídce pro typ zařízení **Wi-Fi** vyberte akci součásti Kontrola zařízení, která se provede při připojení k Wi-Fi: **Povolit** (✓), **Blokovat** (⊘) nebo **Blokovat s výjimkami** (▦).

6. Pokud jste vybrali možnost **Blokovat s výjimkami**, vytvořte seznam důvěryhodných Wi-Fi sítí:

   a. Dvojitým kliknutím otevřete seznam důvěryhodných Wi-Fi sítí.

   b. V bloku **Důvěryhodné Wi-Fi sítě** klikněte na tlačítko **Přidat**.

   c. Tato akce otevře; v tomto okně nakonfigurujte důvěryhodnou Wi-Fi síť (viz obrázek níže):

   - **Síťový název**. Název nebo SSID (Service Set Identifier) Wi-Fi sítě.
   - **Typ ověřování**. Typ ověřování používaný při připojování k Wi-Fi síti.

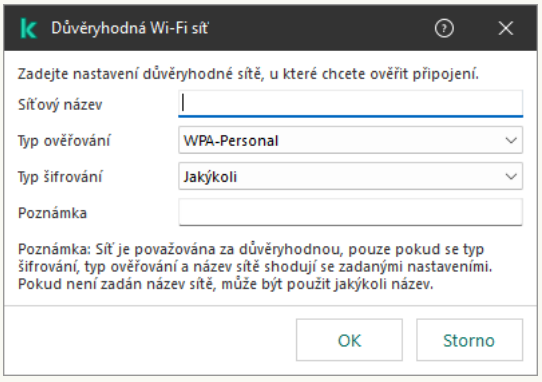
     Počínaje aplikací Kaspersky Endpoint Security pro Windows verze 12.0 byla do aplikace přidána podpora protokolu WPA3. Pokud je na počítači aplikována zásada Kaspersky Endpoint Security verze 12.2, na počítačích s Kaspersky Endpoint Security verze 11.11.0 a starší je vybrán protokol WPA2; WPA2/WPA3 je vybrán pro verze 12.0 až 12.1; WPA3 je vybrán pro verze 12.2 a novější.

   - **Typ šifrování**. Typ šifrování používaný k ochraně provozu Wi-Fi.
   - **Poznámka**. Další informace o přidané Wi-Fi síti.

   Nastavení důvěryhodné Wi-Fi sítě můžete zobrazit v nastavení směrovače.

   Síť Wi-Fi bude považována za důvěryhodnou, pokud se její nastavení budou shodovat se všemi nastaveními určenými v pravidle.

7. Uložte změny.



Nastavení součásti Důvěryhodná Wi-Fi síť

[Jak omezit připojení k Wi-Fi ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Device Control**.
5. V části **Device access rules** vyberte kartu **Devices and Wi-Fi networks**.
   V tabulce jsou uvedena přístupová pravidla pro všechna zařízení, která jsou přítomna v klasifikaci součásti Kontrola zařízení.
6. V bloku **Wi-Fi networks** klikněte na odkaz **Wi-Fi**.
7. V okně, které se otevře, vyberte akci součásti Kontrola zařízení při připojení k Wi-Fi: **Allow**, **Block** nebo **Block with exclusions**.
8. Pokud jste vybrali možnost **Block with exclusions**, vytvořte seznam důvěryhodných Wi-Fi sítí:

   a. Dvojitým kliknutím otevřete seznam důvěryhodných Wi-Fi sítí.

   b. V bloku **Trusted Wi-Fi networks** klikněte na tlačítko **Add**.

   c. Tato akce otevře; v tomto okně nakonfigurujte důvěryhodnou Wi-Fi síť (viz obrázek níže):

- **Name**. Název nebo SSID (Service Set Identifier) Wi-Fi sítě.
- **Authentication type**. Typ ověřování používaný při připojování k Wi-Fi síti.

  Počínaje aplikací Kaspersky Endpoint Security pro Windows verze 12.0 byla do aplikace přidána podpora protokolu WPA3. Pokud je na počítači aplikována zásada Kaspersky Endpoint Security verze 12.2, na počítačích s Kaspersky Endpoint Security verze 11.11.0 a starší je vybrán protokol WPA2; WPA2/WPA3 je vybrán pro verze 12.0 až 12.1; WPA3 je vybrán pro verze 12.2 a novější.

- **Encryption type**. Typ šifrování používaný k ochraně provozu Wi-Fi.
- **Comment**. Další informace o přidané Wi-Fi síti.

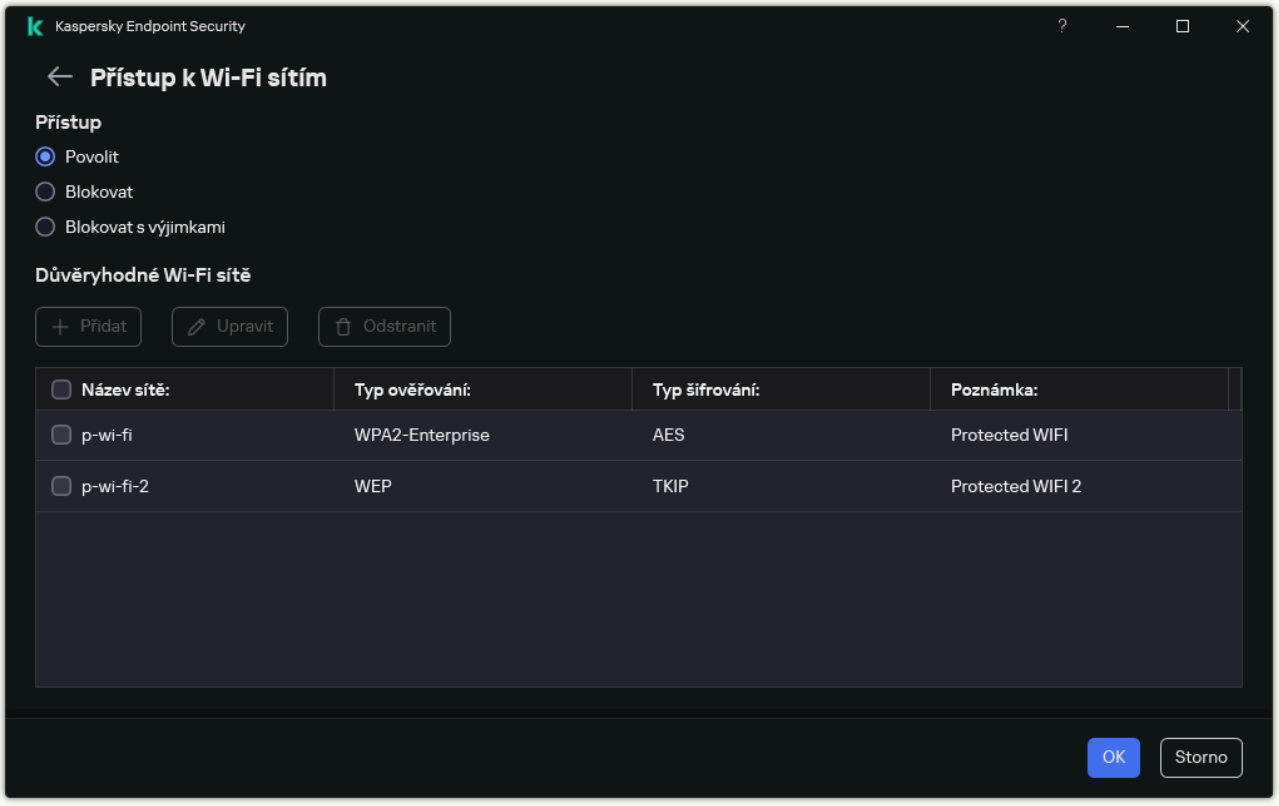
Nastavení důvěryhodné Wi-Fi sítě můžete zobrazit v nastavení směrovače.

Sít Wi-Fi bude považována za důvěryhodnou, pokud se její nastavení budou shodovat se všemi nastaveními určenými v pravidle.

9. Uložte změny.

Jak omezit připojení k Wi-Fi v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola zařízení**.
3. V bloku **Nastavení 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 Wi-Fi sítím** klikněte na odkaz **Wi-Fi**.
   V okně, které se otevře, se zobrazují pravidla přístupu k Wi-Fi síti.



Nastavení přístupu k Wi-Fi

5. V části **Přístup** vyberte akci součásti Kontrola zařízení při připojení k Wi-Fi: **Povolit**, **Blokovat** nebo **Blokovat s výjimkami**.
6. Pokud jste vybrali možnost **Blokovat s výjimkami**, vytvořte seznam důvěryhodných Wi-Fi sítí:
   a. V bloku **Důvěryhodné Wi-Fi sítě** klikněte na tlačítko **Přidat**.

b. Tato akce otevře; v tomto okně nakonfigurujte důvěryhodnou Wi-Fi síť (viz obrázek níže):

- **Název sítě**. Název nebo SSID (Service Set Identifier) Wi-Fi sítě.
- **Typ ověřování**. Typ ověřování používaný při připojování k Wi-Fi síti.

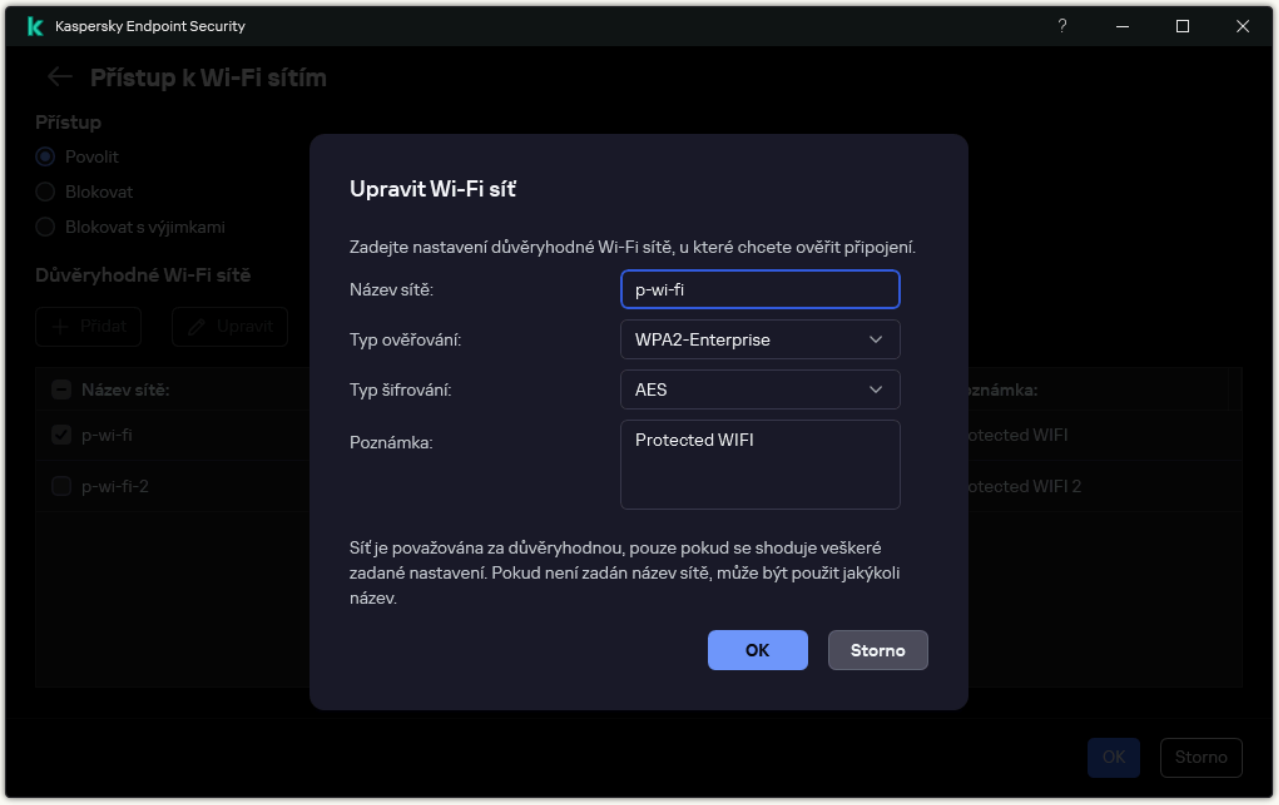
  Počínaje aplikací Kaspersky Endpoint Security pro Windows verze 12.0 byla do aplikace přidána podpora protokolu WPA3. Pokud je na počítači aplikována zásada Kaspersky Endpoint Security verze 12.2, na počítačích s Kaspersky Endpoint Security verze 11.11.0 a starší je vybrán protokol WPA2; WPA2/WPA3 je vybrán pro verze 12.0 až 12.1; WPA3 je vybrán pro verze 12.2 a novější.

- **Typ šifrování**. Typ šifrování používaný k ochraně provozu Wi-Fi.
- **Poznámka**. Další informace o přidané Wi-Fi síti.

Nastavení důvěryhodné Wi-Fi sítě můžete zobrazit v nastavení směrovače.

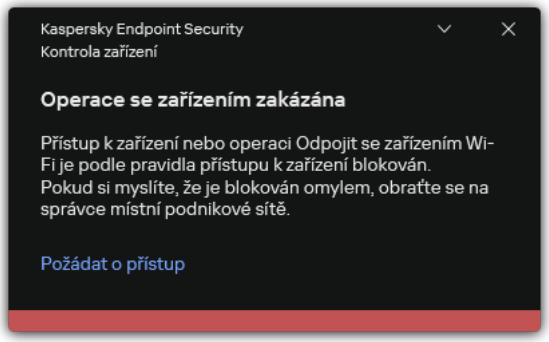
Síť Wi-Fi bude považována za důvěryhodnou, pokud se její nastavení budou shodovat se všemi nastaveními určenými v pravidle.

7. Uložte změny.



Nastavení součásti Důvěryhodná Wi-Fi síť

Výsledkem je, že když se uživatel pokusí připojit k Wi-Fi síti, která není uvedena jako důvěryhodná, aplikace připojení zablokuje a zobrazí upozornění (viz obrázek níže).



Upozornění součásti Kontrola zařízení

Monitorování využití vyměnitelných jednotek

Monitorování využití vyměnitelných jednotek zahrnuje:

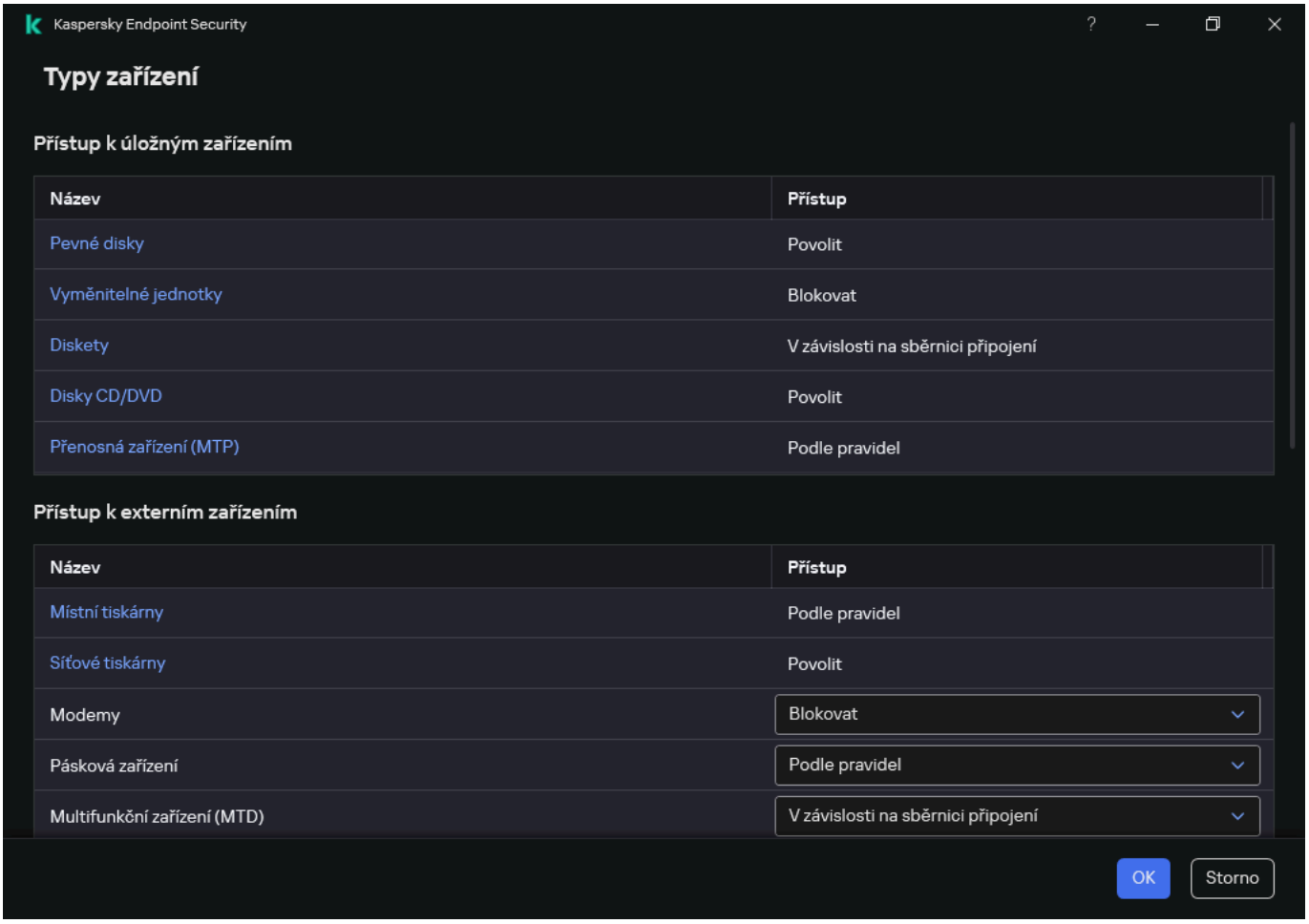
- Monitorování operací se soubory na vyměnitelných jednotkách.
- Monitorování připojování a odpojování důvěryhodných vyměnitelných jednotek.

  Kaspersky Endpoint Security umožňuje monitorovat připojování a odpojování všech důvěryhodných zařízení a nejen vyměnitelných jednotek. Protokolování událostí můžete zapnout v nastavení upozornění pro součást Kontrola zařízení. Události mají stupeň závažnosti *Informační zpráva*.

Postup povolení monitorování využití vyměnitelné jednotky:

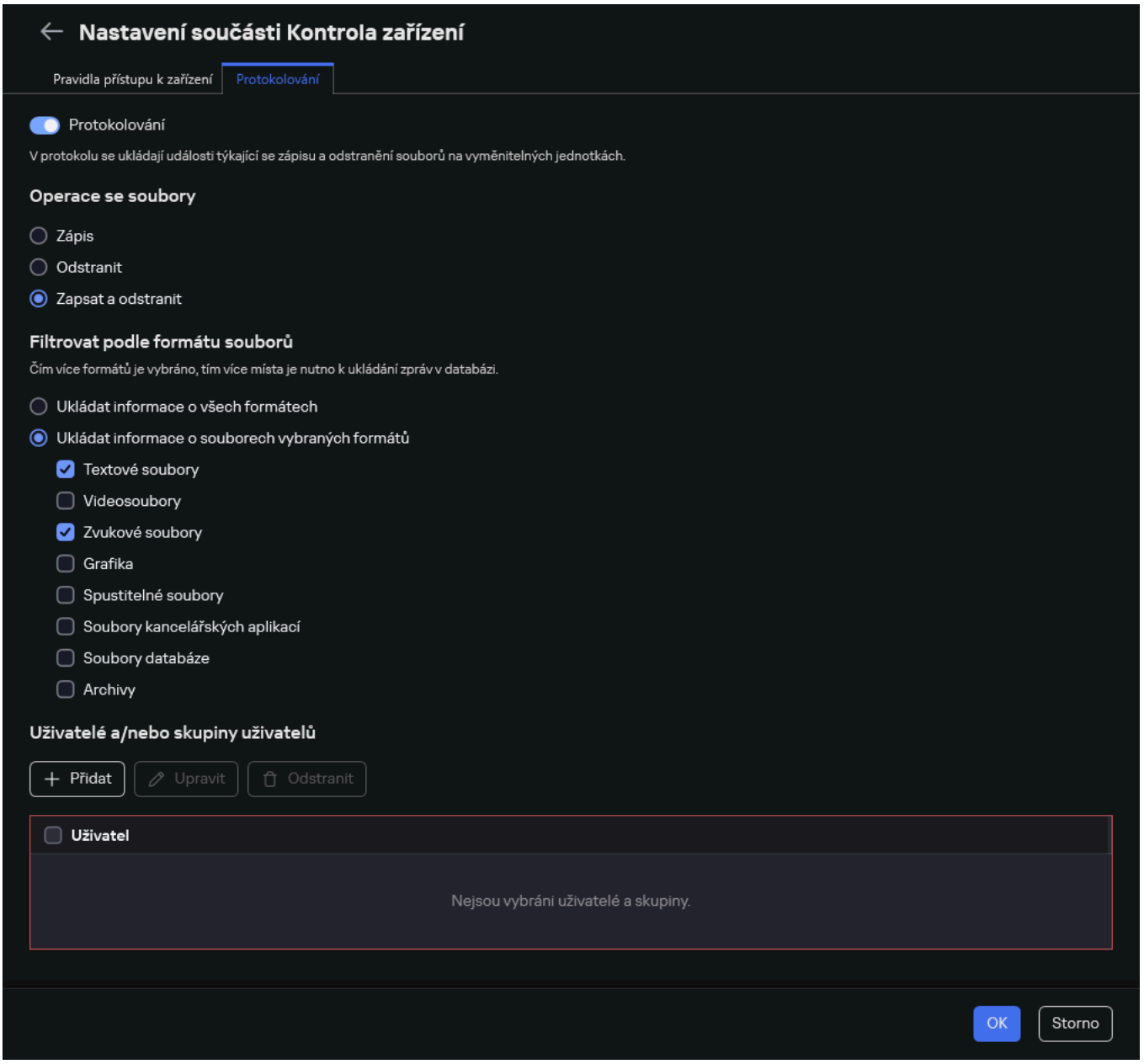
1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola zařízení**.
3. V bloku **Nastavení přístupu** klikněte na tlačítko **Zařízení a Wi-Fi sítě**.

   V okně, které se otevře, se zobrazují pravidla přístupu pro všechna zařízení, která jsou zahrnuta v klasifikaci součásti Kontrola zařízení.



Typy zařízení v součásti Kontrola zařízení

4. V bloku **Přístup k úložným zařízením** vyberte položku **Vyměnitelné jednotky**.
5. V okně, které se otevře, vyberte část **Protokolování**.



Nastavení sledování využití vyměnitelné jednotky

6. Zapněte přepínač **Protokolování**.
7. V bloku **Operace se soubory** vyberte operace, které chcete monitorovat: **Zápis**, **Odstranit**.
8. V bloku **Filtrovat podle formátu souborů** vyberte formáty souborů, jejichž přidružené operace by měla součást Kontrola zařízení monitorovat.
9. Vyberte uživatele nebo skupinu uživatelů, u nichž chcete používání vyměnitelných jednotek monitorovat.
10. 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 **Administration Server** na kartě **Events**. 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
- 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.

Nedoporučujeme přidávat více než 1000 důvěryhodných zařízení, protože to může způsobit nestabilitu systému.

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.

Kaspersky Endpoint Security umožňuje řídit používání důvěryhodných zařízení (připojování a odpojování). Protokolování událostí můžete zapnout v nastavení upozornění pro součást Kontrola zařízení. Události mají stupeň závažnosti *Informační*.

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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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.

   Aplikace Kaspersky Endpoint Security nepodporuje přidávání zařízení z typu **Diskety** na seznam důvěryhodných zařízení.

6. V poli **Poznámka** můžete uvést jakékoli relevantní informace o důvěryhodném zařízení.

7. Vyberte uživatele nebo skupiny uživatelů, kterým chcete povolit přístup k důvěryhodným zařízením.

   Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

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_*`.

Změnu seznamu důvěryhodných zařízení mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Postup přidání zařízení na seznam důvěryhodných zařízení:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
4. V pravé části okna vyberte kartu **Důvěryhodná zařízení**.
5. 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.

6. Klikněte na tlačítko **Přidat** a vyberte způsob přidání zařízení na seznam důvěryhodných zařízení.
7. Chcete-li filtrovat zařízení, vyberte typ zařízení z rozevíracího seznamu **Typ zařízení** (například **Vyměnitelné jednotky**).

Aplikace Kaspersky Endpoint Security nepodporuje přidávání zařízení z typu **Diskety** na seznam důvěryhodných zařízení.

8. 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 **Refresh** prázdný. Chcete-li zobrazit seznam zařízení správně, můžete přidat zařízení podle masky ID zařízení.

9. 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.

10. Klikněte na tlačítko **Refresh**.

    V tabulce se zobrazuje seznam zařízení, která splňují definovaná kritéria filtrování.

11. Zaškrtněte políčko u názvů zařízení, které chcete přidat na seznam důvěryhodných zařízení.

12. Do pole **Poznámka** zadejte popis důvodu přidání zařízení na seznam důvěryhodných zařízení.

13. Klikněte na tlačítko **Select** vpravo od pole **Povolit uživatelům a/nebo skupinám uživatelů**.

14. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

    Ve výchozím nastavení je přístup k důvěryhodným zařízením povolen pro skupinu Všichni.

15. 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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. Uložte soubor.

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. Otevřete soubor.

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 obdrží zprávu s požadavkem v konzole aplikace Kaspersky Security Center.

   Konzola aplikace Kaspersky Security Center má přednastavený výběr událostí *User requests* pro snadné sledování zpráv od uživatelů.
3. 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.
4. Správce aktualizuje nastavení aplikace Kaspersky Endpoint Security v počítači uživatele.

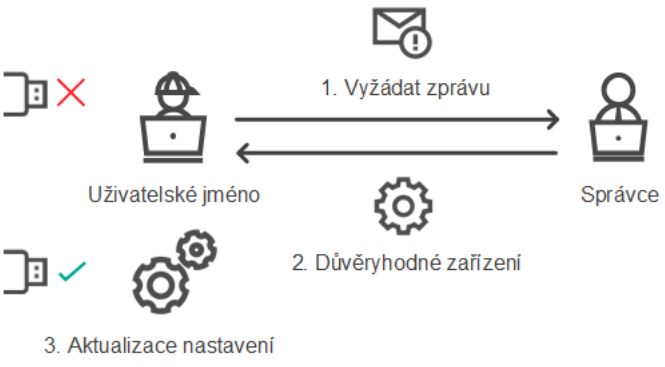


Schéma pro udělení přístupu k zařízení v režimu online

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.

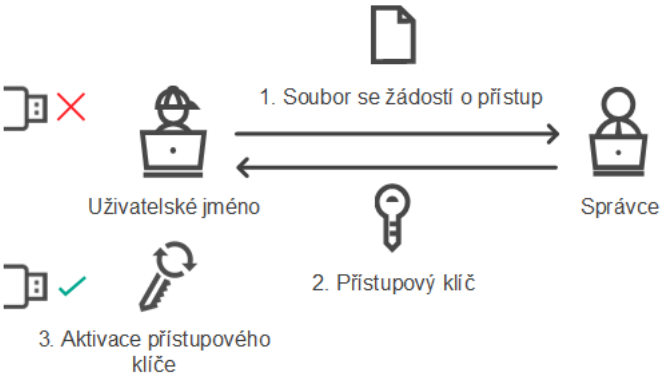


Schéma pro udělení přístupu k zařízení v režimu offline

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:

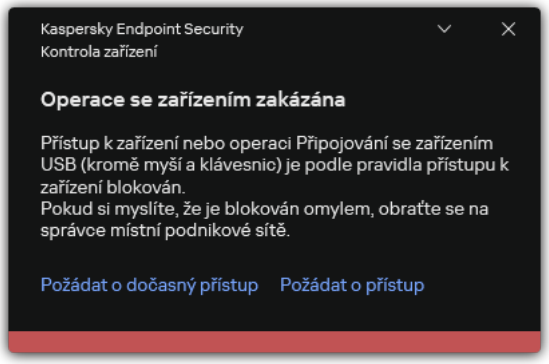
1. Připojte zařízení k počítači.

   Aplikace Kaspersky Endpoint Security zobrazí upozornění, že přístup k zařízení je blokován (viz obrázek níže).

2. Klikněte na odkaz **Požádat o přístup**.

   Tím otevřete okno se zprávou správci. Tato zpráva obsahuje informace o blokovaném zařízení.

3. Klikněte na tlačítko **Odeslat**.



Upozornění součásti Kontrola zařízení

Poté správce obdrží v konzole aplikace Kaspersky Security Center událost *Zpráva o blokování přístupu k zařízení určená pro správce*. Událost obsahuje uživatelské jméno, název počítače, podrobnosti o zařízení, ke kterému se uživatel pokouší získat přístup, a další informace. Můžete nakonfigurovat, jakým způsobem bude správce o těchto událostech informován, například zvolit upozornění e-mailem. Konzola aplikace Kaspersky Security Center má přednastavený výběr událostí *User requests* pro snadné sledování zpráv od uživatelů.

Pokud chcete povolit přístup, musíte přidat zařízení na seznam důvěryhodných. Po aktualizaci nastavení aplikace Kaspersky Endpoint Security v počítači může uživatel získat přístup k 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 obsahující seznam připojených zařízení.

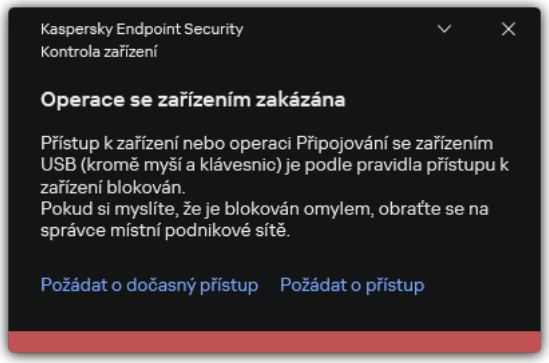
3. V seznamu připojených zařízení vyberte to, ke kterému chcete získat přístup.

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

Jak může správce vytvořit přístupový klíč pro blokované zařízení 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. V seznamu klientských počítačů vyberte počítač uživatele, který potřebuje získat dočasný přístup k blokovanému zařízení.
5. V kontextové nabídce počítače vyberte položku **Udělit přístup v offline režimu**.
6. Tím otevřete okno; v tomto okně 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.

Jak může administrátor vytvořit přístupový klíč pro blokované zařízení ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. V seznamu klientských počítačů vyberte počítač uživatele, který potřebuje získat dočasný přístup k blokovanému zařízení.
3. Klikněte na tlačítko se třemi tečkami (•••) nad seznamem počítačů a poté klikněte na tlačítko **Grant access to the device in offline mode**.

4. V okně, které se otevře, vyberte část **Device Control**.
5. Klikněte na tlačítko **Browse** a stáhněte soubor se žádostí o přístup přijatý od uživatele.

   Zobrazí se informace o blokovaném zařízení, ke kterému uživatel žádá o přístup.
6. V případě potřeby změňte hodnotu nastavení **Access duration (hours)**.

   Ve výchozím nastavení **Access duration (hours)** přebírá hodnotu udanou uživatelem při vytváření souboru se žádostí o přístup.
7. Zadejte časové období, během kterého lze na zařízení aktivovat přístupový klíč.

   Toto nastavení určuje časové období, během kterého může uživatel aktivovat přístup k zablokovanému zařízení pomocí poskytnutého přístupového klíče.
8. 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola zařízení**.
3. V bloku **Žádost o přístup** klikněte na tlačítko **Žádost 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.

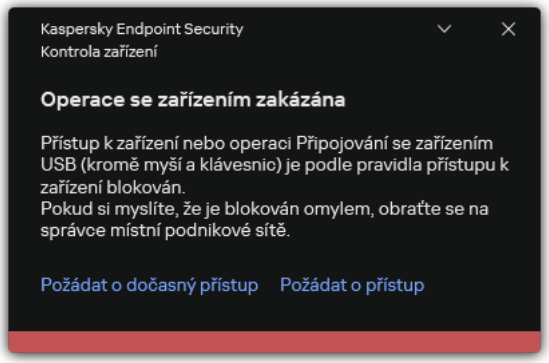
   Otevře se okno obsahující informace o poskytnutí přístupu.
6. Klikněte na tlačítko **OK**.

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. Odborníci Kaspersky poskytují uživateli šablonu zprávy popisující důvody, proč byl přístup k zařízení zablokován (viz obrázek níže).

Pro správu šablon zprávy jsou k dispozici speciální proměnné (např. `%USER_NAME%`). Proměnné umožňují použití jedné šablony zprávy pro různé počítače. Při generování zprávy aplikace Kaspersky Endpoint Security načte hodnotu proměnné z nastavení operačního systému a vloží ji do zprávy odpovídající konkrétnímu počítači, uživateli a události.



Upozornění součásti Kontrola 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. K tomu musí uživatel kliknout na tlačítko **Požádat o přístup** nebo **Požádat o dočasný přístup** a odeslat zprávu s popisem situace správci. Můžete si také připravit šablonu zprávy pro správce a přidat k ní údaje, které mohou informovat o vašem rozhodnutí povolit nebo zablokovat přístup k zařízení. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k zařízení určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Jak změnit šablonu zprávy součásti Kontrola webu v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
4. V bloku **Nastavení šablony zprávy** klikněte na tlačítko **Šablony**.
5. Otevře se okno, ve kterém nakonfigurujte šablony součásti Kontrola aplikací:
   - **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 pro správce**. 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.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Proměnná** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Můžete také obnovit výchozí text šablony.
6. Uložte změny.

Jak změnit šablonu zprávy součásti Kontrola zařízení ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Device Control**.
5. V bloku **Message templates** nakonfigurujte šablony pro zprávy součásti Kontrola aplikací:
   - **Message to user**. 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.
   - **Message to administrator**. 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.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Add variable** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Můžete také obnovit výchozí text šablony.
6. Uložte změny.

Jak změnit šablonu zprávy součásti Kontrola zařízení v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. V bloku **Šablony zpráv** nakonfigurujte šablony pro zprávy součásti Kontrola aplikací:
   - **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.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Přidat proměnnou** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Můžete také obnovit výchozí text šablony.

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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola zařízení**.
3. V bloku **Nastavení přístupu** 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 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 netypického 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 **Rule triggers in Smart Training state**.

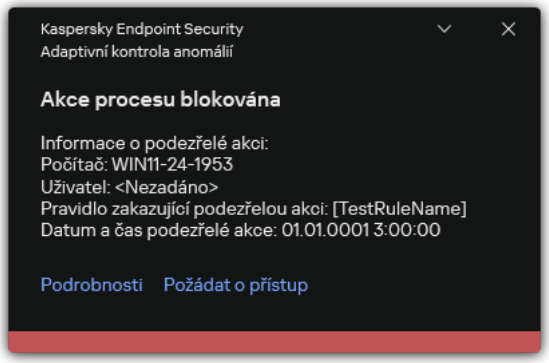
2. Analýza zprávy o aktivaci pravidel.

   Správce analyzuje zprávu o aktivaci pravidel nebo obsah úložiště **Rule triggers in Smart Training state**. 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 se konfiguruje v reálném čase 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 **Rule triggers in Smart Training state**. Doporučujeme přečíst si zprávu o aktivaci pravidel a obsahu úložiště **Rule triggers in Smart Training state**.

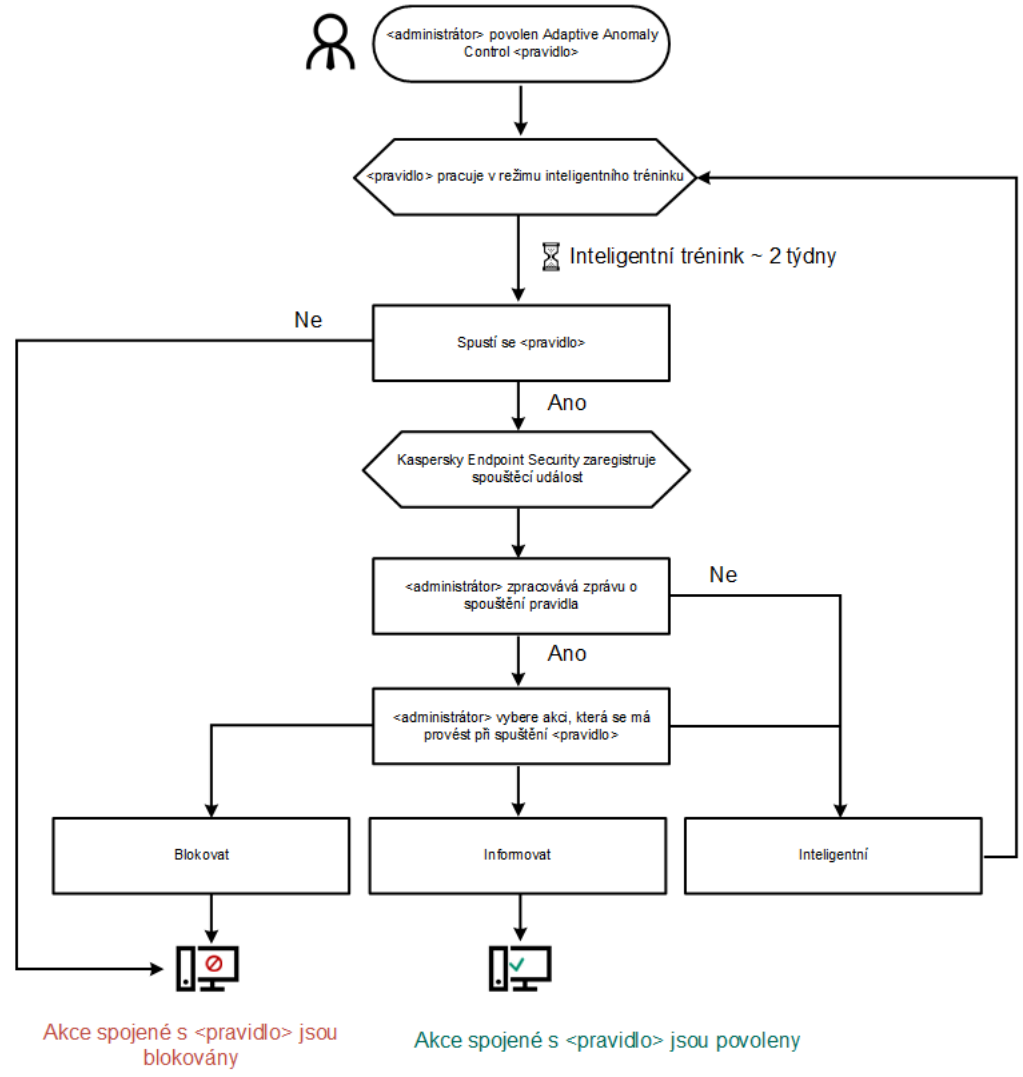
Pokud se škodlivá aplikace pokusí provést akci, aplikace Kaspersky Endpoint Security akci zablokuje a zobrazí upozornění (viz obrázek níže).



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

Zkušební režim součásti Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií zahrnuje sadu pravidel (vzorů chování). 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. Součást Adaptivní kontrola anomálií neblokuje aktivitu aplikací v počítači, ale pouze informuje správce. Můžete také ručně vybrat akci, která se provede při spuštění pravidla součásti Adaptivní kontrola anomálií.

Jak zobrazit seznam pravidel součásti Adaptivní kontrola anomálií v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Security Controls → Adaptive Anomaly Control**.
5. Zaškrtněte políčko **Adaptivní kontrola anomálií**.
6. V části **Nastavení pravidel součásti Adaptivní kontrola anomálií** se podívejte na seznam pravidel.
   Ve výchozím nastavení všechna pravidla fungují v režimu **Inteligentní**.
7. V případě potřeby potvrďte aktualizaci pravidla součásti Adaptivní kontrola anomálií.
8. V případě potřeby vyberte akci při spuštění pravidla součásti Adaptivní kontrola anomálií:
   - **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.

9. V případě potřeby zakažte pravidla, která nechcete použít.
10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak zobrazit pravidla součásti Adaptivní kontrola anomálií ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Adaptive Anomaly Control**.
5. Zapněte přepínač **Adaptive Anomaly Control ENABLED**.
6. V části **Rules** se podívejte na seznam pravidel.
   Ve výchozím nastavení všechna pravidla fungují v režimu **Smart**.
7. V případě potřeby potvrďte aktualizaci pravidla součásti Adaptivní kontrola anomálií.
8. V případě potřeby vyberte akci při spuštění pravidla součásti Adaptivní kontrola anomálií:
   - **Block**. 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.
   - **Inform**. 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.
9. V případě potřeby zakažte pravidla, která nechcete použít.
10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak zobrazit seznam pravidel součásti Adaptivní kontrola anomálií v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Security Controls** → **Adaptive Anomaly Control**.
3. Zapněte přepínač **Adaptivní kontrola anomálií**.
4. V bloku **Pravidla** klikněte na odkaz **Upravit pravidla**.
   Otevře se seznam pravidel součásti Adaptivní kontrola anomálií. Ve výchozím nastavení všechna pravidla fungují v režimu **Inteligentní**.
5. V případě potřeby potvrďte aktualizaci pravidla součásti Adaptivní kontrola anomálií.
6. V případě potřeby vyberte akci při spuštění pravidla součásti Adaptivní kontrola anomálií:
   - **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. V případě potřeby zakažte pravidla, která nechcete použít.
8. Uložte změny.

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 se během trénování pravidlo nikdy nespustilo, součást Adaptivní kontrola anomálií považuje takové chování za atypické a změní stav pravidla na **Inteligentní blokování**. Následně aplikace zablokuje veškerou aktivitu, která vyhovuje tomuto pravidlu.

Pokud se pravidlo spustí během trénování, musíte ručně nakonfigurovat akci, kterou aplikace použije u zjištěné aktivity, která odpovídá tomuto pravidlu. Pokud při spuštění pravidla akci nevyberete, součást Adaptivní kontrola anomálií bude pokračovat v trénovacím režimu.

Povolení a zakázání pravidla součásti Adaptivní kontrola anomálií

Postup povolení a zakázání pravidla součásti Adaptivní kontrola anomálií:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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 *Spuštění prostředí Microsoft PowerShell z aplikace sady Office*).
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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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 stavu 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 **Rule triggers in Smart Training state** administračního serveru Kaspersky Security Center. Po skončení časového období nastaveného pro práci v chytrém zkušebním stavu 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 než 1 000 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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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.

   Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   > 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://<object>` kde `<object>` 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://<command>`, 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 a import výjimek pro pravidla součásti Adaptivní kontrola anomálií

Postup exportu nebo importu seznamu výjimek pro vybraná pravidla:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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. Uložte soubor.

5. 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. Otevřete soubor.

Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML 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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **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.

Pro zprávy pro správce o blokování potenciálně škodlivých akcí jsou k dispozici zvláštní šablony. Pro správu šablon zprávy jsou k dispozici speciální proměnné (např. `%USER_NAME%`). Proměnné umožňují použití jedné šablony zprávy pro různé počítače. Při generování zprávy aplikace Kaspersky Endpoint Security načte hodnotu proměnné z nastavení operačního systému a vloží ji do zprávy odpovídající konkrétnímu počítači, uživateli a události.

Postup úpravy šablony zprávy:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.

3. V bloku **Šablony** nakonfigurujte šablony pro zprávy součásti Adaptivní kontrola anomálií:

- **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. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování aktivity aplikace určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Přidat proměnnou** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

Výchozí text šablony můžete také obnovit pomocí tlačítka **Obnovit**.

4. Uložte změny.

Sledování operací součásti Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií zahrnuje několik nástrojů pro monitorování. Hlavním účelem monitorování součásti Adaptivní kontrola anomálií je konfigurace součásti během trénování.

Zprávy součásti Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií používá následující zprávy:

- **Zpráva o stavu pravidel součásti Adaptivní kontrola anomálií**. Zpráva obsahuje informace o stavu pravidel součásti Adaptivní kontrola anomálií (*Off*, *Smart Training*, *Smart Block*, *Notify*, *Block*). Tato zpráva umožňuje analyzovat úroveň tréninku součásti Adaptivní kontrola anomálií a vyhodnotit počet pravidel, která byla převedena z režimu *Smart Training* na normální provozní režim (například *Smart Block*).

- **Zpráva o aktivovaných pravidlech součásti Adaptivní kontrola anomálií**. Zpráva obsahuje informace o aktivacích pravidel. Zpráva také zobrazuje režim spouštění pravidel: *Block* (včetně pravidla *Smart Block*) nebo *Notify*. Tyto zprávy umožňují vyhodnotit aktivitu součásti Adaptivní kontrola anomálií v počítačích uživatelů.

Jak zobrazit zprávy součásti Adaptivní kontrola anomálií v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení → Adaptivní kontrola anomálií**.
4. Proveďte jednu z následujících akcí:
   - Chcete-li zkontrolovat zprávu o stavu pravidel součásti Adaptivní kontrola anomálií, klikněte na odkaz **Zpráva o stavu pravidel součásti Adaptivní kontrola anomálií**.
   - Chcete-li zkontrolovat zprávu o aktivovaných pravidlech součásti Adaptivní kontrola anomálií, klikněte na odkaz **Zpráva o aktivovaných pravidlech součásti Adaptivní kontrola anomálií**.
5. Spustí se proces generování zprávy.

Zpráva se zobrazí v novém okně.

Jak zobrazit zprávy součásti Adaptivní kontrola anomálií ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls → Adaptive Anomaly Control**.
5. V bloku **Rules** proveďte některou z následujících akcí:
   - Chcete-li zkontrolovat zprávu o stavu pravidel součásti Adaptivní kontrola anomálií, vyberte možnost **View report → Rules state**.
   - Chcete-li zkontrolovat zprávu o spuštěných pravidlech součásti Adaptivní kontrola anomálií, klikněte na tlačítko **View report → Detections**.
6. Spustí se proces generování zprávy.

Zpráva se zobrazí v novém okně.

Chcete-li generovat zprávy v konzole aplikace Kaspersky Security Center, musíte povolit přenos dat na server pro správu. Přenos dat je ve výchozím nastavení povolen.

Jak povolit přenos dat součásti Adaptivní kontrola anomálií do konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Zprávy a úložiště**.
4. V bloku **Přenos dat na server pro správu** klikněte na tlačítko **Nastavení**.
5. Zaškrtněte následující políčka:
   - **Zpráva o stavu pravidel součásti Adaptivní kontrola anomálií**.
   - **Zpráva o aktivovaných pravidlech součásti Adaptivní kontrola anomálií**.
6. Uložte změny.

Jak povolit přenos dat u součásti Adaptivní kontrola anomálií ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **KSC Integration**.
5. V části **Data transfer to Administration Server** zaškrtněte následující políčka:
   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.
6. Uložte změny.

Úložiště Rule triggers in Smart Training state

V trénovacím režimu odešle součást Adaptivní kontrola anomálií informace o spuštěných pravidlech do samostatného úložiště, **Rule triggers in Smart Training state**. Informace o aktivovaných pravidlech jsou v úložišti reprezentovány jako seznam událostí. Chcete-li vyladit součást Adaptivní kontrola anomálií, můžete buď potvrdit atypické chování v počítači, nebo přidat výjimku z pravidla.

Události součásti Adaptivní kontrola anomálií

Součást Adaptivní kontrola anomálií protokoluje události spuštění pravidla v režimech *Block* (včetně *Smart Block*) a *Notify*. Pro tento účel jsou poskytovány následující události:

Process action blocked

Process action skipped

Události obsahují informace o podezřelé aktivitě, včetně kontrolních součtů souborů, zúčastněných uživatelů, času aktivace pravidla a názvu počítače. Po analýze události můžete okamžitě přidat výjimky z pravidla, pokud považujete aktivitu za legitimní.

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* nebo jiná kategorie), 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. Správce může vytvořit mnoho pravidel. Jedna aplikace může splňovat kritéria více pravidel. Priorita pravidla blokování je vyšší než priorita pravidla povolení. Kaspersky Endpoint Security při každém spuštění zkontroluje, zda aplikace splňuje pravidlo. Aplikace Kaspersky Endpoint Security postupně porovnává aplikaci se všemi pravidly součásti Kontrola aplikací.

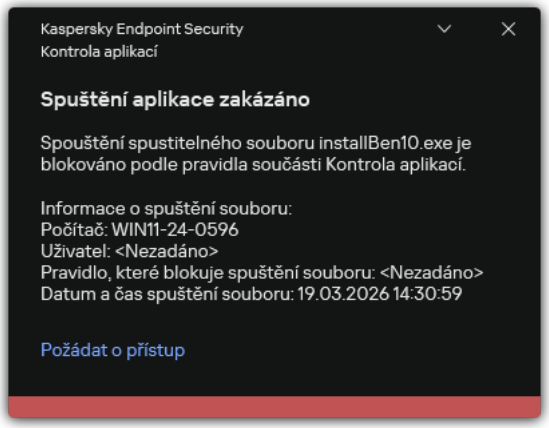
3. Volba režimu součásti Kontrola aplikací.

   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.

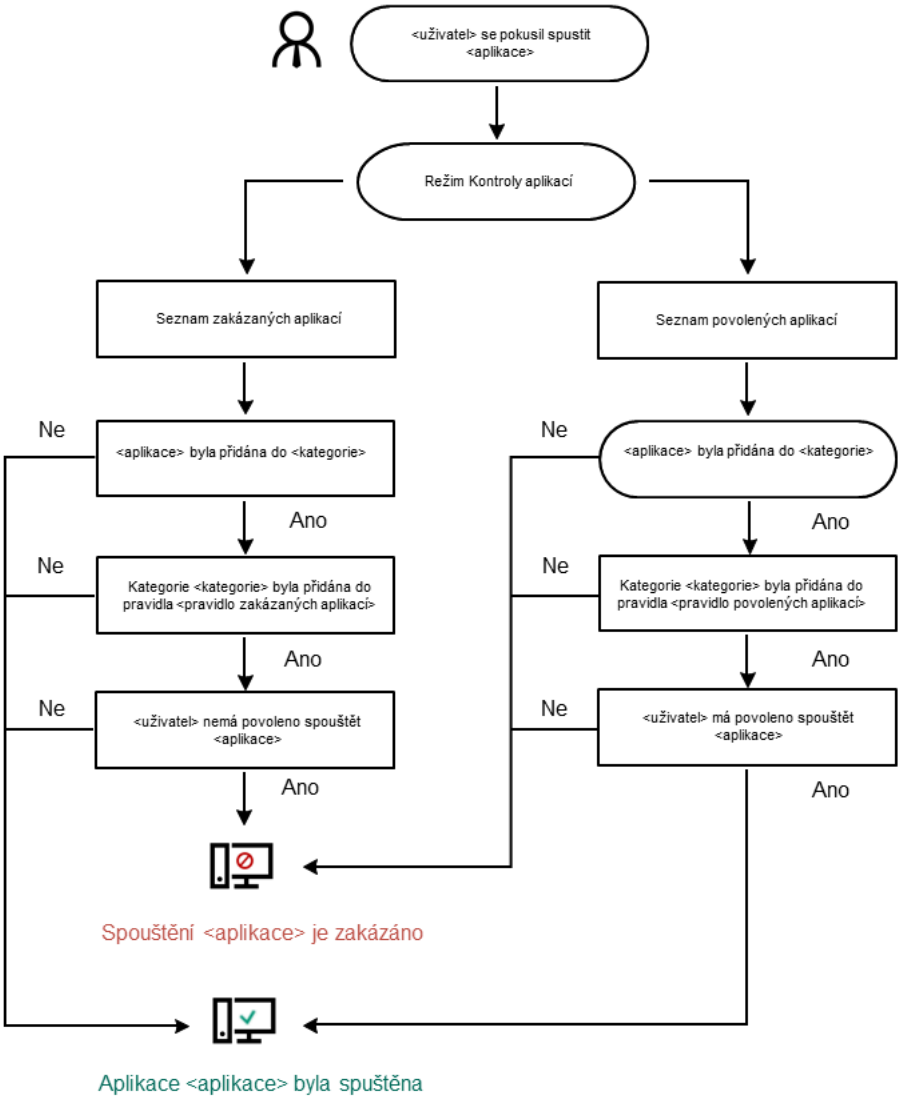
  Pravidla součásti Kontrola aplikací vytvořená v konzole pro správu aplikace Kaspersky Security Center jsou založena na vašich vlastních kategoriích aplikací, nikoli na podmínkách zahrnutí a vyloučení, jako je tomu v místním rozhraní aplikace Kaspersky Endpoint Security.

- 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.
- 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, které aplikace Kaspersky Endpoint Security označuje jako kategorii KL **Ostatní software\Aplikace, důvěryhodné podle reputace v KSN** / Applications, trusted according to reputation in KSN, se může lišit v závislosti na tom, zda je k dispozici připojení k serverům 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

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.

Zobrazení informací o aplikaci

Informace o nainstalovaných aplikacích poskytuje Kaspersky Security Center Network Agent. Informace o nainstalovaných aplikacích jsou k dispozici v konzole aplikace Kaspersky Security Center Network Agent ve složce **Applications registry**. Součást Network Agent aktualizuje informace při každé synchronizaci s aplikací Kaspersky Security Center. Podrobnosti o informacích odesílaných součástí Network Agent najdete v nápovědě k aplikaci Kaspersky Security Center.

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 **Advanced** → **Application management** → **Applications registry**.
3. Vyberte aplikaci.
4. V kontextové nabídce aplikace vyberte možnost **Properties**.

Zobrazení informací o spustitelných souborech

Můžete snížit zatížení databáze při dotazech na informace o spustitelných souborech. Chcete-li toho dosáhnout, doporučujeme spustit úlohu *Inventarizace* na několika referenčních počítačích, které mají nainstalovanou vaši standardní sadu softwaru.

Seznam spustitelných souborů můžete získat pomocí úlohy *Inventarizace* aplikace Kaspersky Endpoint Security. Seznam spustitelných souborů můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Executable files**.

Před spuštěním úlohy *Inventarizace* se ujistěte, že databáze splňuje doporučení aplikace Kaspersky Security Center. Podrobnosti o omezeních pro databáze najdete v nápovědě k aplikaci Kaspersky Security Center.

Jak spustit úlohu Inventarizace v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Inventarizace**.

Krok 2. Rozsah inventarizace

Vytvořte seznam složek, ve kterých má Kaspersky Endpoint Security hledat spustitelné soubory. Nakonfigurujte nastavení inventarizace (viz tabulka níže).

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. Výběr účtu pro spuštění úlohy

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

Krok 5. Konfigurace plánu spuštění úlohy

Nakonfigurujte plán úloh, například ručně.

Krok 6. Definování názvu úlohy

Zadejte název úlohy, například *Základní inventarizace*.

Krok 7. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy. Prohledávání spustitelných souborů je tak v počítačích uživatelů prováděno podle nakonfigurovaného plánu.

[Jak spustit úlohu Inventarizace ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Inventory**.
   c. Do pole **Task name** zadejte krátký popis, například *Základní inventarizace*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Chcete-li nakonfigurovat úlohu, přejděte na vlastnosti úlohy (viz tabulka níže).
8. Zaškrtněte políčko vedle úlohy.
9. Klikněte na tlačítko **Start**.
   Můžete sledovat stav úlohy a počet zařízení, ve kterých byla úloha úspěšně dokončena nebo dokončena s chybou. Spustitelné soubory tak budou vyhledávány v počítačích uživatelů podle určeného plánu.

Nastavení inventarizace

Parametr	Popis
Inventory scope	Seznam objektů, které budou tvořit rozsah inventarizace.
DLL modules inventory	Kaspersky Endpoint Security vyhledá v rozsahu inventarizace moduly DLL a odešle informace do aplikace Kaspersky Security Center. Povolení inventáře modulů DLL výrazně prodlouží dobu potřebnou k dokončení úlohy Inventarizace a zvýší velikost databáze.
Script files inventory	Kaspersky Endpoint Security vyhledá v rozsahu inventarizace skripty a odešle informace do aplikace Kaspersky Security Center. Povolení inventáře souborů skriptu výrazně prodlouží dobu potřebnou k dokončení úlohy Inventarizace a zvýší velikost databáze.
Run only when the computer is idle	Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.
Scan only new and modified files	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.

Skip file that is scanned for longer than (sec) N s	Omezení doby provádění úlohy. Po zadané době aplikace Kaspersky Endpoint Security úlohu ukončí. Úloha není označena jako dokončená. Až Kaspersky Endpoint Security příště úlohu spustí, bude spuštěna od začátku a podle plánu.
Scan archives	Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).
Scan distribution packages	Kontrola distribučních balíčků aplikací třetích stran.
Do not unpack large compound files	Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí. Aplikace kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.

Postup otevření okna vlastností u spustitelného souboru ve složce Executable files:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly pro správu vyberte možnosti **Advanced** → **Application management** → **Executable files**.
3. Vyberte spustitelný soubor.
4. V kontextové nabídce spustitelného souboru vyberte možnost **Properties**.

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**.

Aktualizace informací o nainstalovaných aplikacích a spustitelných souborech

Od verze 12.3 aplikace Kaspersky Endpoint Security pro systém Windows bylo optimalizováno fungování součásti Kontrola aplikací s databází spustitelných souborů. Kaspersky Endpoint Security 12.3 pro systém Windows po odstranění souboru z počítače automaticky aktualizuje databázi. To umožňuje udržovat databázi aktuální a šetřit prostředky aplikace Kaspersky Security Center.

Aby byla databáze nainstalovaných aplikací aktuální, musí být povoleno odesílání informací o aplikaci na server pro správu (tj. ve výchozím nastavení povoleno).

Jak povolit odesílání informací o aplikaci v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Zprávy a úložiště**.
4. V bloku **Přenos dat na server pro správu** klikněte na tlačítko **Nastavení**.
5. Zaškrtněte políčko **Spuštěné aplikace**.
6. Uložte změny.

Jak povolit odesílání informací o aplikaci prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **KSC Integration**.
5. V bloku **Data transfer to Administration Server** klikněte na tlačítko **Advanced settings**.
6. V okně, které se otevře, zaškrtněte políčko **About started applications**.
7. Uložte změny.

Jak povolit režim Blokované aplikace

Blokované aplikace je režim, ve kterém umožňuje Kontrola aplikací uživatelům spouštět všechny aplikace kromě aplikací, které jsou v jejích pravidlech zakázány. To znamená, že pokud žádné pravidlo odepřít neexistuje, součást Kontrola aplikací povolí spuštění aplikace. Tento režim je ve výchozím nastavení povolen.

Před povolením režimu *Blokované aplikace* doporučujeme otestovat pravidla součásti Kontrola aplikací. Za tímto účelem můžete povolit testovací režim.

Jak vybrat režim Blokované aplikace v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Kontrolní prvky zabezpečení → Kontrola aplikací**.
5. Zaškrtněte políčko **Kontrola aplikací**.
6. V bloku **Nastavení součásti Kontrola aplikací** pomocí rozevíracího seznamu **Režim kontroly aplikací** vyberte možnost **Seznam blokovaných položek**.
7. V rozevíracím seznamu **Akce** vyberte akci pro součást Kontrola aplikací:
   - **Otestovat pravidla**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.
   - **Použít pravidla**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.
8. Vyberte stav pro pravidla součásti Kontrola aplikací:
   - **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.
   - **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.

   Pokud je třeba, přidejte nová pravidla součásti Kontrola aplikací.
9. Nakonfigurujte rozšířená nastavení součásti Kontrola aplikací:
   - **Monitorovat zavádění modulů DLL (výrazně zvýší zatížení systému)**. 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 „**Golden Image\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.
   - **Používat přísné ověřování digitálního podpisu**. Jako aktivující podmínku pro pravidlo součásti Kontrola aplikací můžete vybrat certifikát. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané pouze pomocí certifikátů z úložiště důvěryhodných systémových certifikátů. Aplikace podepsané takovým certifikátem jsou také považovány za důvěryhodné součástmi ochrany, například úlohou *Kontrola malwaru*. Pokud však v pravidlu součásti Kontrola aplikací zadáte certifikát z jiného úložiště, aplikace Kaspersky Endpoint Security takové pravidlo nepoužije.

     Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané certifikátem z úložiště Trusted Root Certificate Store systému Windows. Takové aplikace nejsou součástí důvěryhodné zóny. Součásti ochrany monitorují aktivitu těchto aplikací.

- **Zpráva o blokování**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.
- **Zpráva pro správce**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit režim Blokované aplikace ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **App Control**.
5. Zapněte přepínač **Application Control ENABLED**.
6. V bloku **Operating mode** vyberte položku **Block all except the rules list**.
7. V bloku **Action** vyberte akci pro součást Kontrola aplikací:
   - **Inform**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.
   - **Apply rules**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.
8. Vyberte stav pro pravidla součásti Kontrola aplikací:
   - **Enabled**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo použito.
   - **Disabled**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo ignorováno.
   - **Test mode**. 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.

   Pokud je třeba, přidejte nová pravidla součásti Kontrola aplikací.
9. Nakonfigurujte rozšířená nastavení součásti Kontrola aplikací:
   - **Monitor loading of DLL modules**. 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 „**Golden Image\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.
   - **Use strict digital signature verification**. Jako aktivující podmínku pro pravidlo součásti Kontrola aplikací můžete vybrat certifikát. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané pouze pomocí certifikátů z úložiště důvěryhodných systémových certifikátů. Aplikace podepsané takovým certifikátem jsou také považovány za důvěryhodné součástmi ochrany, například úlohou *Kontrola malwaru*. Pokud však v pravidlu součásti Kontrola aplikací zadáte certifikát z jiného úložiště, aplikace Kaspersky Endpoint Security takové pravidlo nepoužije.

     Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané certifikátem z úložiště Trusted Root Certificate Store systému Windows. Takové aplikace nejsou součástí důvěryhodné zóny. Součásti ochrany monitorují aktivitu těchto aplikací.
   - **Message to user**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.

- **Message to administrator**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit režim Blokované aplikace v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Zapněte přepínač **Kontrola aplikací**.
4. V bloku **Režim kontroly spouštění aplikací** vyberte položku **Seznam zakázaných aplikací. Jsou povoleny všechny aplikace kromě aplikací v seznamu pravidel**.
5. V bloku **Akce při spuštění aplikací blokovaných pravidly** vyberte akci pro součást Kontrola aplikací:
   - **Informovat (testovací režim) a zaznamenávat události do protokolu ve zprávě**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.
   - **Blokovat**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.
6. Vyberte stav pro pravidla součásti Kontrola aplikací:
   - **Povoleno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo použito.
   - **Zakázáno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo ignorováno.
   - **Režim testování**. 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.

   Pokud je třeba, přidejte nová pravidla součásti Kontrola aplikací.
7. Nakonfigurujte rozšířená nastavení součásti Kontrola aplikací:
   - **Monitorovat zavádění modulů 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 „**Golden Image\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.
   - **Používat přísné ověřování digitálního podpisu**. Jako aktivující podmínku pro pravidlo součásti Kontrola aplikací můžete vybrat certifikát. Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané pouze pomocí certifikátů z úložiště důvěryhodných systémových certifikátů. Aplikace podepsané takovým certifikátem jsou také považovány za důvěryhodné součástmi ochrany, například úlohou *Kontrola malwaru*. Pokud však v pravidlu součásti Kontrola aplikací zadáte certifikát z jiného úložiště, aplikace Kaspersky Endpoint Security takové pravidlo nepoužije.

     Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané certifikátem z úložiště Trusted Root Certificate Store systému Windows. Takové aplikace nejsou součástí důvěryhodné zóny. Součásti ochrany monitorují aktivitu těchto aplikací.
   - **Šablony zpráv o blokování aplikace**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.
   - **Šablona textu zprávy, která se zobrazí, pokud je spuštění aplikace blokováno**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.
8. Uložte změny.

Součást Kontrola aplikací tak blokuje zablokované aplikace. Kaspersky Endpoint Security také generuje události *Spuštění aplikace zakázáno*. Tyto události můžete použít ke generování zprávy *Report on prohibited applications* v konzole aplikace Kaspersky Security Center. V souhrnu zprávy můžete zobrazit seznam aplikací a počítačů, u kterých bylo spuštěno pravidlo součásti Kontrola aplikací.

Kontrola aplikací založená na počítači se základním stavem

Počítač se základním stavem můžete použít k vytvoření bitové kopie se sadou aplikací, které potřebujete. Tuto bitovou kopii pak můžete použít k nasazení operačního systému a aplikací do jiných počítačů. Ne vždy je možné udržovat bitovou kopii aktuální. Kontrola aplikací umožňuje udržovat seznam povolených aplikací na základě počítače se základním stavem. Kontrola aplikací automaticky určí, které aplikace jsou nainstalovány v počítači se základním stavem, a aktualizuje kategorii. Počítače tak získají aktuální seznam povolených aplikací.

Konfigurace součásti Kontrola aplikací na základě počítače se základním stavem zahrnuje následující kroky:

1. Vytváří se kategorie automatických aktualizací. Při vytváření nové kategorie vyberte kategorii **Category that includes executable files from a specific folder** a vyberte svůj výchozí počítač.

   Jak vytvořit automaticky aktualizovanou kategorii v konzole pro správu (MMC)

   1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
   2. Ve stromu konzoly pro správu vyberte možnosti **Advanced** → **Application management** → **Application categories**.
   3. V pracovním prostoru klikněte na tlačítko **New category**.
      Spustí se průvodce vytvořením kategorie aplikace.
   4. Postupujte podle pokynů průvodce vytvořením kategorie aplikace.

   Krok 1. Volba typu kategorie

   Vyberte **Category that includes executable files from selected devices** jako typ kategorie.

   Krok 2. Zadání názvu kategorie uživatelů

   V tomto kroku určete název kategorie aplikací.

   Krok 3. Nastavení

   Tento krok je k dispozici v případě, že jste vybrali typ kategorie **Category that includes executable files from selected devices**.

   V tomto krok klikněte na tlačítko **Add** a zadejte počítače, jejichž spustitelné soubory budou přidány aplikací Kaspersky Security Center do kategorie aplikace. Všechny spustitelné soubory z určených počítačů přítomné ve složce **Executable files** budou aplikací Kaspersky Security Center přidány do kategorie aplikací.

   V tomto kroku můžete také nakonfigurovat následující nastavení:

   - Algoritmus pro výpočet hashovací funkce. Chcete-li vybrat algoritmus, je nutné zaškrtnout alespoň jedno z následujících políček:
     - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
     - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
   - Zaškrtávací políčko **Synchronize data with 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 **Executable files**.
     Pokud není zaškrtnuto políčko **Synchronize data with Administration Server repository**, aplikace Kaspersky Security Center neprovede žádné úpravy kategorie aplikací po jejím vytvoření.

   Krok 4. Filtr

   V tomto kroku nakonfigurujte filtr souborů.

   Můžete určit typ souboru, který chcete použít pro vytvoření kategorie aplikace.

   - **All files**. Kategorie bude odpovídat všem souborům. Tato možnost je nastavena jako výchozí.
   - **Only files outside the application categories**. Kategorie bude odpovídat pouze souborům mimo kategorie aplikací.

Můžete určit složky vybraných počítačů, které obsahují soubory, které chcete použít pro vytvoření kategorie aplikace.

- **All folders**. Kategorie bude odpovídat všem složkám. Tato možnost je nastavena jako výchozí.
- **Specified folder**. Kategorie bude odpovídat pouze zadané složce. Pokud vyberete tuto možnost, musíte určit cestu ke složce.

Krok 5. Vytvoření vlastní kategorie

Ukončete průvodce.

Jak vytvořit kategorii s automaticky přidávaným obsahem ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Operations** → **Third-party applications** → **Application categories**.
   Tím otevřete seznam kategorií aplikace.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce vytvořením kategorie aplikace.
3. Nakonfigurujte obecné nastavení kategorie aplikace:
   - Název kategorie.
   - Způsob vytváření kategorie. Vyberte **Category that includes executable files from selected devices** jako typ kategorie.

   Přejděte k dalšímu kroku.
4. Nakonfigurujte rozšířená nastavení kategorie aplikace:
   - Určete počítače, ze kterých bude Kaspersky Security Center přidávat spustitelné soubory do této kategorie aplikace. Všechny spustitelné soubory z určených počítačů přítomné ve složce **Executable files** budou aplikací Kaspersky Security Center přidány do kategorie aplikací.
   - Vyberte algoritmus pro výpočet hashovací funkce.
   - Nakonfigurujte interval pro synchronizaci dat s úložištěm serveru pro správu.
   - Nakonfigurujte filtr pro soubory.
5. Ukončete průvodce.

Při vytváření automaticky aktualizované kategorie může být výhodné soubory dále rozdělit do více kategorií. Například soubory operačního systému a soubory ze složky Program Files. K tomu můžete použít filtr v nastavení kategorií a vybrat jednotlivé složky.

2. Volba režimu součásti Kontrola aplikací. Je třeba zabránit spouštění všech aplikací, které nejsou výslovně povoleny. To provedete tak, že vyberete režim *Blokované aplikace*.
3. Vytvoření pravidla součásti Kontrola aplikací. V nastavení pravidel vyberte kategorii, do které patří spustitelné soubory z počítače se základním stavem.

   Jak konfigurovat součást Kontrola aplikací na základě počítače se základním stavem v konzole pro správu (MMC)

   1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
   2. Ve stromu konzoly vyberte možnost **Policies**.
   3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
   4. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
   5. Zaškrtněte políčko **Kontrola aplikací**.
   6. V bloku **Nastavení součásti Kontrola aplikací** pomocí rozevíracího seznamu **Režim kontroly aplikací** vyberte možnost **Seznam blokovaných položek**.
   7. V rozevíracím seznamu **Akce** vyberte akci pro součást Kontrola aplikací:
      - **Otestovat pravidla**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.

- **Použít pravidla**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.

8. V seznamu pravidel součásti Kontrola aplikací klikněte na tlačítko **Přidat**.
   Spustí se průvodce přidáním aplikace do pravidla součásti Kontrola aplikací.
9. V rozevíracím seznamu **Kategorie** vyberte automaticky aktualizovanou kategorii na základě počítače se základním stavem.
10. Vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo součásti Kontrola aplikací.
11. Nakonfigurujte rozšířená nastavení pravidla Kontrola aplikací:
    - **Zamítnout pro ostatní uživatele**. Aplikace brání spouštění aplikací, které patří do vybrané kategorie, všem uživatelům, kteří nejsou v seznamu.
    - **Důvěryhodné nástroje aktualizace**. Aplikace Kaspersky Endpoint Security vyhodnocuje aplikace obsažené ve vybrané kategorii aplikací jako důvěryhodné aktualizační nástroje s oprávněním vytvořit jiné spustitelné soubory, kterým bude následně povoleno spuštění.
12. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak konfigurovat součást Kontrola aplikací na základě počítače se základním stavem ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **App Control**.
5. Zapněte přepínač **Application Control ENABLED**.
6. V bloku **Operating mode** vyberte položku **Block all except the rules list**.
7. V bloku **Action** vyberte akci pro součást Kontrola aplikací:
   - **Inform**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.
   - **Apply rules**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.
8. V seznamu pravidel součásti Kontrola aplikací klikněte na tlačítko **Add**.
   Spustí se průvodce přidáním aplikace do pravidla součásti Kontrola aplikací.
9. V části **Categories/Applications** vyberte automaticky aktualizovanou kategorii na základě počítače se základním stavem.
10. Vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo součásti Kontrola aplikací.
11. Nakonfigurujte rozšířená nastavení pravidla Kontrola aplikací:
    - **Users**. Aplikace brání spouštění aplikací, které patří do vybrané kategorie, všem uživatelům, kteří nejsou v seznamu.
    - **Trusted Updaters**. Aplikace Kaspersky Endpoint Security vyhodnocuje aplikace obsažené ve vybrané kategorii aplikací jako důvěryhodné aktualizační nástroje s oprávněním vytvořit jiné spustitelné soubory, kterým bude následně povoleno spuštění.
12. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak konfigurovat součást Kontrola aplikací na základě počítače se základním stavem v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. Zapněte přepínač **Kontrola aplikací**.
4. V bloku **Režim kontroly spouštění aplikací** vyberte položku **Seznam zakázaných aplikací. Jsou povoleny všechny aplikace kromě aplikací v seznamu pravidel**.

5. V bloku **Akce při spuštění aplikací blokovaných pravidly** vyberte akci pro součást Kontrola aplikací:

   - **Informovat (testovací režim) a zaznamenávat události do protokolu ve zprávě**. Kontrola aplikací neblokuje aplikace, kterým pravidla brání ve spuštění, ale generuje události o spouštění aplikací, které by jinak byly zablokovány.
   - **Blokovat**. Kontrola aplikací blokuje zablokované aplikace a generuje příslušné události.

6. V seznamu pravidel součásti Kontrola aplikací klikněte na tlačítko **Přidat**.

   Spustí se průvodce přidáním aplikace do pravidla součásti Kontrola aplikací.

7. V části **Kategorie** vyberte automaticky aktualizovanou kategorii na základě počítače se základním stavem.
8. Vyberte uživatele nebo skupiny uživatelů, na které chcete použít pravidlo součásti Kontrola aplikací.
9. Nakonfigurujte rozšířená nastavení pravidla Kontrola aplikací:

   - **Zamítnout pro ostatní uživatele**. Aplikace brání spouštění aplikací, které patří do vybrané kategorie, všem uživatelům, kteří nejsou v seznamu.
   - **Důvěryhodné nástroje aktualizace**. Aplikace Kaspersky Endpoint Security vyhodnocuje aplikace obsažené ve vybrané kategorii aplikací jako důvěryhodné aktualizační nástroje s oprávněním vytvořit jiné spustitelné soubory, kterým bude následně povoleno spuštění.

10. Uložte změny.

Správa pravidel součásti Kontrola aplikací

Aplikace Kaspersky Endpoint Security kontroluje pomocí 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 výjimek.* 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.

Pokud jste vybrali certifikát jako podmínku aktivace pravidla, musíte zajistit, aby byl tento certifikát přidán do důvěryhodného systémového úložiště v počítači, a zkontrolovat nastavení využití důvěryhodného systémového úložiště v aplikaci.

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:

- **Povoleno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo použito.
- **Zakázáno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo ignorováno.
- **Režim testování**. 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 podmínky aktivace pro pravidlo součásti Kontrola 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 v konzole pro správu:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly pro správu vyberte možnosti **Advanced** → **Application management** → **Application categories**.
3. V pracovním prostoru klikněte na tlačítko **New category**.
   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:

- Category with content added manually. Data of executable files is manually added to the category Pokud jste vybrali tento typ kategorie, v kroku *Configuring conditions for inclusion of applications in categories* a kroku *Configuring conditions for exclusion of applications from categories* budete moci určit kritéria, podle nichž budou spustitelné soubory automaticky zahrnuty do příslušné kategorie.
- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category Pokud jste vybrali tento typ kategorie, v kroku *Settings* budete moci určit počítač, jehož spustitelné soubory budou automaticky zahrnuty do příslušné kategorie.
- Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category Pokud jste vybrali tento typ kategorie, v kroku *Repository folder* 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

Při přidání velkého počtu podmínek do pravidel součásti Kontrola aplikací (například hodnoty hash souborů) se zvýší spotřeba prostředků počítače. Když celkový počet podmínek dosáhne 50 000, může dojít k problémům s výkonem. Za účelem optimalizace výkonu se doporučuje zkontrolovat a snížit počet podmínek.

Tento krok je k dispozici v případě, že jste vybrali typ kategorie **Category with content added manually**.

V tomto kroku vyberte v rozevíracím seznamu **Add** 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 the files in the 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 the files from the 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 **Certificate fingerprint**.

- **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 the files from the 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.
- **From KL category**. 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 *Office Applications* zahrnuje aplikace ze sady Microsoft Office, aplikaci Adobe Acrobat a další.

  Můžete vybrat všechny kategorie KL a vygenerovat rozšířený seznam důvěryhodných aplikací.

- **Specify path to application (masks supported)**. V klientském zařízení vyberte složku. Aplikace Kaspersky Security Center přidá spustitelné soubory z této složky do vlastní kategorie.
- **Select certificate from 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 **Certificate fingerprint**.

  Můžete si vybrat úložiště certifikátů. Ve výchozím nastavení součást Kontrola aplikací používá pravidla pouze pro aplikace podepsané certifikátem z důvěryhodného systémového úložiště certifikátů. To je umožněno zaškrtávacím políčkem **Používat přísné ověřování digitálního podpisu**.

- **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 k dispozici v případě, že jste vybrali typ kategorie **Category with content added manually**.

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 **Add** 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 the files in the 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 the files from the 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 the files from the 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.
- **From KL category**. 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 *Office Applications* zahrnuje aplikace ze sady Microsoft Office, aplikaci Adobe Acrobat a další.

  Můžete vybrat všechny kategorie KL a vygenerovat rozšířený seznam důvěryhodných aplikací.
- **Specify path to application (masks supported)**. V klientském zařízení vyberte složku. Aplikace Kaspersky Security Center přidá spustitelné soubory z této složky do vlastní kategorie.
- **Select certificate from 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 **Category that includes executable files from selected devices**.

V tomto krok klikněte na tlačítko **Add** a zadejte počítače, jejichž spustitelné soubory budou přidány aplikací Kaspersky Security Center do kategorie aplikace. Všechny spustitelné soubory z určených počítačů přítomné ve složce **Executable files** budou aplikací Kaspersky Security Center přidány do kategorie aplikací.

V tomto kroku můžete také nakonfigurovat následující nastavení:

- Algoritmus pro výpočet hashovací funkce. Chcete-li vybrat algoritmus, je nutné zaškrtnout alespoň jedno z následujících políček:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- Zaškrtávací políčko **Synchronize data with 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 **Executable files**.

  Pokud není zaškrtnuto políčko **Synchronize data with Administration Server repository**, aplikace Kaspersky Security Center neprovede žádné úpravy kategorie aplikací po jejím vytvoření.

Krok 6. Složka úložiště

Tento krok je k dispozici v případě, že jste vybrali typ kategorie **Category that includes executable files from a specific folder**.

V tomto kroku 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 pro výpočet hashovací funkce. Chcete-li vybrat algoritmus, je nutné zaškrtnout alespoň jedno z následujících políček:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- 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 interval (1–168 hours)**. 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.

  Pole je dostupné v případě, že je zaškrtnuto políčko **Force folder scan for changes**.

Krok 7. Vytvoření vlastní kategorie

Ukončete průvodce.

Postup přidání nové podmínky aktivace pro pravidlo součásti Kontrola aplikací v rozhraní aplikace:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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: N** nebo kartu **Výjimky: N** 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 k souboru nebo složce**.
   - **Podmínky „kategorie KL“**. 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.
   - **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 (vyměnitelná jednotka)**. 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 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 k souboru nebo složce**.
7. Uložte změny.

Při přidávání podmínek vezměte v úvahu následující zvláštní aspekty součásti Kontrola aplikací:

- Kaspersky Endpoint Security podporuje znaky `*` a `?` pro zadání masky v metadatech: **File name**, **Application name**, **Vendor**.
- 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 certifikátu**. 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**.

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 konzoly pro správu vyberte možnosti **Advanced** → **Application management** → **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**.

5. V okně, které se otevře, postupujte takto:

   - V horní části okna vyberte jednu z následujících možností:
     - **Add to a new application category**. Tuto možnost vyberte, pokud chcete vytvořit novou kategorii aplikací a přidat do ní spustitelné soubory.
     - **Add to an existing application category**. Tuto možnost vyberte, pokud chcete vybrat stávající kategorii aplikací a přidat do ní spustitelné soubory.
   - V bloku **Rule type** vyberte některou z následujících možností:
     - **Rules for adding to inclusions**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která do kategorii aplikací přidá spustitelné soubory.
     - **Rules for adding to exclusions**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která z kategorie aplikací vyloučí spustitelné soubory.
   - V bloku **Parameter used as a condition** vyberte některou z následujících možností:
     - **Certificate details (or SHA256 hashes for files without a certificate)**.
     - **Certificate details (files without a certificate will be skipped)**.
     - **Only SHA256 (files without a hash will be skipped)**.
     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

6. Uložte změny.

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** stromu konzole pro správu vyberte kartu **Events**.

3. V rozevíracím seznamu **Event selections** 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**.

7. V okně, které se otevře, nakonfigurujte nastavení kategorie aplikace:

   - V horní části okna vyberte jednu z následujících možností:
     - **Add to a new application category**. Tuto možnost vyberte, pokud chcete vytvořit novou kategorii aplikací a přidat do ní spustitelné soubory.
     - **Add to an existing application category**. Tuto možnost vyberte, pokud chcete vybrat stávající kategorii aplikací a přidat do ní spustitelné soubory.
   - V bloku **Rule type** vyberte některou z následujících možností:
     - **Rules for adding to inclusions**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která do kategorii aplikací přidá spustitelné soubory.
     - **Rules for adding to exclusions**. Tuto možnost vyberte, pokud chcete vytvořit podmínku, která z kategorie aplikací vyloučí spustitelné soubory.
   - V bloku **Parameter used as a condition** vyberte některou z následujících možností:
     - **Certificate details (or SHA-256 hashes for files without a certificate)**.
     - **Certificate details (files without a certificate will be skipped)**.
     - **Only SHA-256 (files without a hash will be skipped)**.
     - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

8. Uložte změny.

Přidání pravidla součásti Kontrola aplikací

Přidání pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.
4. Klikněte na tlačítko **Přidat**.
   Otevře se okno **Pravidlo součásti Kontrola aplikací**.
5. 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**.
     c. Upravte nastavení vybrané kategorie aplikací.
     d. Uložte změny.
     e. V rozevíracím seznamu **Kategorie** vyberte vytvořenou kategorii aplikací, na základě které chcete vytvořit pravidlo.
6. V tabulce **Uživatelé a jejich práva** klikněte na tlačítko **Přidat**.
   Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
7. V tabulce **Uživatelé a jejich práva** postupujte takto:
   - 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 **Blokovat** na příslušných řádcích.
8. Zaškrtněte políčko **Zamítnout pro ostatní uživatele**, pokud chcete, aby všem uživatelům, kteří nejsou ve sloupci **Uživatel nebo skupina** a nejsou součástí skupiny uživatelů zadané ve sloupci **Uživatel nebo skupina**, bylo zakázáno spouštět aplikace patřící do vybrané kategorie.
9. 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.

10. Uložte změny.

Přidání nebo úprava pravidla součásti Kontrola aplikací:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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**.

   Kliknutím na toto tlačítko otevřete okno s nastavením pravidla součásti Kontrola 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. V tabulce **Uživatelé a jejich práva** klikněte na tlačítko **Přidat**.

   Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.

   Pravidlo standardně platí pro všechny uživatele.

   > Pokud v tabulce není zadán žádný uživatel, pravidlo nelze uložit.

   d. V tabulce **Uživatelé a jejich práva** pomocí přepínače definujte právo uživatelů spouštět aplikace.

   e. Zaškrtněte políčko **Zamítnout pro ostatní uživatele**, pokud chcete, aby aplikace zabránila spuštění aplikací, které splňují podmínky pro aktivaci pravidla, všem uživatelům, kteří nejsou uvedeni v tabulce **Uživatelé a jejich práva** a nejsou členy skupin uživatelů uvedených v tabulce **Uživatelé a jejich práva**.

   > Pokud není políčko **Zamítnout pro ostatní uživatele** zaškrtnuté, aplikace Kaspersky Endpoint Security nekontroluje spouštění aplikací uživateli, kteří nejsou zadáni v tabulce **Uživatelé a jejich práva** a nepatří do skupiny uživatelů zadaných v tabulce **Uživatelé a jejich práva**.

   f. Pokud chcete, aby aplikace Kaspersky Endpoint Security považovala aplikace vyhovující podmínkám spouštění pravidla za důvěryhodné nástroje aktualizace, zaškrtněte políčko **Důvěryhodné nástroje aktualizace**. *Důvěryhodné nástroje aktualizace* jsou aplikace, které mají povoleno vytvářet další spustitelné soubory, které budou moci následně spouštět.

   Pokud aplikace spouští více pravidel, Kaspersky Endpoint Security nastaví příznak *Důvěryhodné nástroje aktualizace*, pokud jsou splněny následující podmínky:

   - Všechna pravidla umožňují spuštění aplikace.
   - Alespoň jedno pravidlo má zaškrtnuto políčko **Důvěryhodné nástroje aktualizace**.

6. Na kartě **Podmínky: N** vytvořte nebo upravte seznam podmínek zahrnutí pro spuštění pravidla.

7. Na kartě **Výjimky: N** 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.

Změna stavu pravidla součásti Kontrola aplikací pomocí aplikace Kaspersky Security Center

Postup změny stavu pravidla součásti Kontrola aplikací v konzole pro správu:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Kontrolní prvky zabezpečení → Kontrola aplikací**.

   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.

4. Ve sloupci **Stav** kliknutím levým tlačítkem zobrazte 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.
   - **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.

5. Uložte změny.

Postup změny stavu pravidla součásti Kontrola aplikací v rozhraní aplikace:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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:
   - **Povoleno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo použito.
   - **Zakázáno**. Tento stav označuje, že při spuštění součásti Kontrola aplikací bude příslušné pravidlo ignorováno.
   - **Režim 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.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení → Kontrola aplikací**.
4. 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. Uložte soubor.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
5. Postup importu 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. Otevřete soubor.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.
6. 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 **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **App Control**.
5. V části **Operating mode** vyberte seznam pravidel: seznam zakázaných nebo povolených aplikací.
6. Postup exportu seznamu pravidel:
   a. Vyberte pravidla, která chcete exportovat.
   b. Klikněte na tlačítko → **Export**.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru JSON ve výchozí složce pro stahování.
7. Postup importu seznamu pravidel:
   a. Klikněte na tlačítko → **Import**.
      V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam pravidel.
   b. Otevřete soubor.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.
8. Uložte změny.

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** stromu konzole pro správu vyberte kartu **Events**.
3. Klikněte na tlačítko **Create a selection**.
4. V okně, které se otevře, přejděte do části **Events**.
5. Klikněte na tlačítko **Clear all**.
6. V tabulce **Events** zaškrtněte políčko **Spuštění aplikace zakázáno**.
7. Uložte změny.
8. V rozevíracím seznamu **Event selections** 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 New Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V kroku **Selecting the report template type** vyberte možnost **Other** → **Report on prohibited 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. 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.

Povolení a zakázání testování pravidel součásti Kontrola aplikací

Postup povolení nebo zakázání testování pravidel součásti Kontrola aplikací v Kaspersky Security Center:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.

   V pravé části okna se zobrazí nastavení součásti Kontrola aplikací.
4. 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 libovolnou aplikaci 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.
5. Proveďte jednu z následujících akcí:

   - Chcete-li povolit testování pravidel součásti Kontrola aplikací, v rozevíracím seznamu **Akce** vyberte možnost **Otestovat pravidla**.
   - Pokud chcete povolit součásti Kontrola aplikací správu spouštění aplikací na uživatelských počítačích, v rozevíracím seznamu vyberte **Použít pravidla**.
6. Uložte změny.

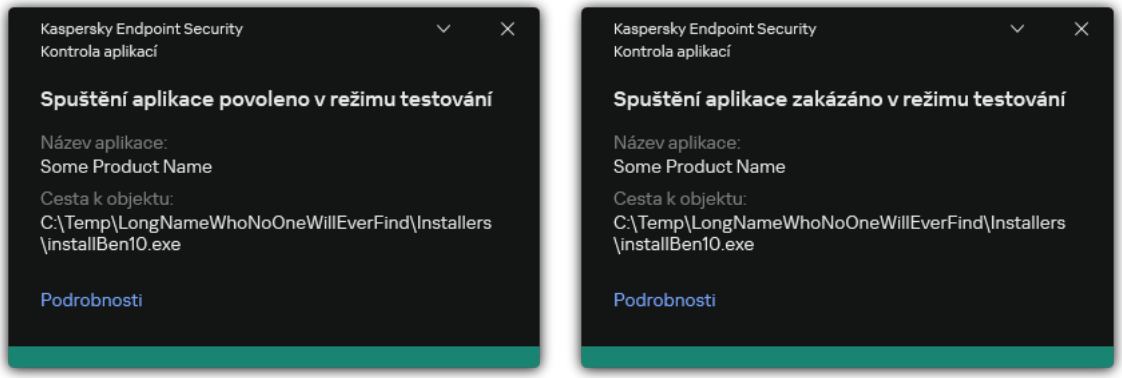
Postup povolení testování pravidel součásti Kontrola aplikací nebo výběru akce blokování u součásti Kontrola aplikací:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **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** vyberte možnost **Režim 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.

Aplikace Kaspersky Endpoint Security nebude blokovat aplikace, jejichž spouštění je zakázáno součástí Kontrola aplikací, ale odešle upozornění o jejich spuštění na administrační server. Můžete také konfigurovat zobrazování upozornění o testování pravidel na počítači uživatele (viz obrázek níže).



Upozornění součásti Kontrola aplikací v testovacím režimu

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 New Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V kroku **Selecting the report template type** vyberte možnost **Other → Report on prohibited 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 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** stromu konzole pro správu vyberte kartu **Events**.
3. Klikněte na tlačítko **Create a selection**.
4. V okně, které se otevře, přejděte do části **Events**.
5. Klikněte na tlačítko **Clear all**.
6. Na kartě **Events** zaškrtněte políčka **Spuštění aplikace zakázáno v režimu testování** a **Spuštění aplikace povoleno v režimu testování**.
7. Uložte změny.
8. V rozevíracím seznamu **Event selections** vyberte vytvořený výběr.
9. Klikněte na tlačítko **Run selection**.

Monitor aktivity aplikací

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.

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 v části **Monitorování** klikněte na dlaždici **Monitor aktivity 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.

Pokud chcete skrýt informace o aktivitě aplikace v počítači uživatele, můžete uživateli omezit přístup k nástroji Monitor aktivity aplikací.

Jak skrýt Monitor aktivity aplikací v rozhraní aplikace pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Rozhraní**.
4. Pomocí zaškrtávacího políčka **Skrýt část Monitor aktivity aplikací** udělíte nebo zrušíte přístup k nástroji.
5. Uložte změny.

Jak skrýt Monitor aktivity aplikací v rozhraní aplikace pomocí webové konzoly a konzoly pro správu

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **User Interaction**.
5. Pomocí zaškrtávacího políčka **Hide Application Activity Monitor section** udělíte nebo zrušíte přístup k nástroji.
6. Uložte změny.

Pravidla pro vytváření masek názvů pro soubory nebo složky

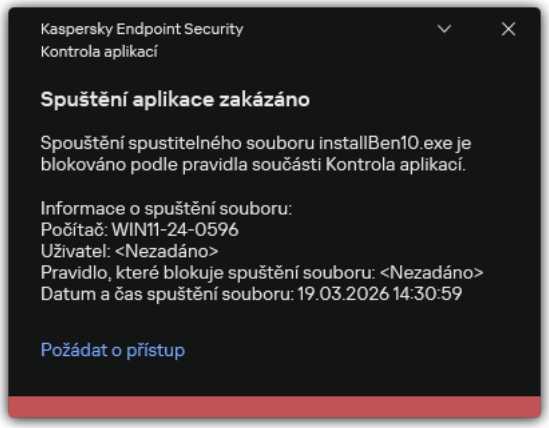
Maska názvu souboru nebo složky reprezentuje názvy složek nebo názvy a přípony souborů, v nichž jsou použity určité společné znaky.

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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, 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. Odborníci Kaspersky poskytují uživateli šablonu zprávy popisující důvody, proč byla aplikace zablokována (viz obrázek níže). Pro správu šablon zprávy jsou k dispozici speciální proměnné (např. `%USER_NAME%`). Proměnné umožňují použití jedné šablony zprávy pro různé počítače. Při generování zprávy aplikace Kaspersky Endpoint Security načte hodnotu proměnné z nastavení operačního systému a vloží ji do zprávy odpovídající konkrétnímu počítači, uživateli a události.



Upozornění součásti Kontrola aplikací

Pokud se uživatel domnívá, že spuštění dané aplikace bylo zablokováno omylem, může pomocí odkazu ve zprávě odeslat zprávu místnímu podnikovému správci sítě. K tomu musí uživatel kliknout na tlačítko **Požádat o přístup** a odeslat zprávu s popisem situace správci. Můžete si také připravit šablonu zprávy pro správce a přidat k ní údaje, které mohou informovat o vašem rozhodnutí povolit nebo zablokovat přístup k aplikaci. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování spuštění aplikace určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Jak upravit šablonu zprávy součásti Kontrola aplikací v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
4. V bloku **Nastavení šablony zprávy** klikněte na tlačítko **Šablony**.
5. Otevře se okno, ve kterém nakonfigurujte šablony součásti Kontrola aplikací:
   - **Zpráva o blokování**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.

     Šablony zpráv pro součásti Kontrola aplikací nemůžete konfigurovat v testovacím režimu. Kontrola aplikací v testovacím režimu zobrazuje přednastavená upozornění.
   - **Zpráva pro správce**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Proměnná** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Výchozí text šablony můžete také obnovit pomocí tlačítka **Výchozí režim**.
6. Uložte změny.

Jak upravit šablonu zprávy součásti Kontrola aplikací ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **App Control**.
5. V bloku **Message templates** klikněte na odkaz **Messages about application startup block** a nakonfigurujte šablony pro zprávy součásti Kontrola aplikací:
   - **Message to user**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.

     Šablony zpráv pro součásti Kontrola aplikací nemůžete konfigurovat v testovacím režimu. Kontrola aplikací v testovacím režimu zobrazuje přednastavená upozornění.

- **Message to administrator**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Add variable** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

Výchozí text šablony můžete také obnovit pomocí tlačítka **Reset to default**.

6. Uložte změny.

Jak upravit šablonu zprávy součásti Kontrola aplikací v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola aplikací**.
3. V bloku **Šablony zpráv o blokování aplikace** nakonfigurujte šablony pro zprávy součásti Kontrola aplikací:
   - **Zpráva o blokování**. Šablonu zprávy, která se zobrazí při spuštění pravidla kontroly aplikací blokujícího spuštění aplikace.

     Šablony zpráv pro součásti Kontrola aplikací nemůžete konfigurovat v testovacím režimu. Kontrola aplikací v testovacím režimu zobrazuje přednastavená upozornění.
   - **Zpráva správci**. Šablona zprávy, kterou může uživatel odeslat správci podnikové sítě LAN, pokud se uživatel domnívá, že aplikace byla omylem zablokována.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Přidat proměnnou** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Výchozí text šablony můžete také obnovit pomocí tlačítka **Obnovit**.
4. Uložte změny.

Proměnné v šablonách zpráv součásti Kontrola aplikací

V šablonách zpráv uživatelů nebo šablon zpráv správce můžete použít následující proměnné:

- **Název aktivovaného pravidla** – `%RULE%`.

  Název pravidla, které zablokovalo spuštění souboru.
- **Aktuální datum** – `%DATE%`.

  Datum zablokování provádění souboru ve formátu DD.MM.RRRR.
- **Aktuální čas** – `%TIME%`.

  Čas, kdy bylo zablokováno spuštění souboru, ve formátu HH:MM.
- **Uživatelské jméno** – `%USER_NAME%`.

  Název aktuálního uživatelského účtu v počítači, na kterém bylo spuštění souboru zablokováno, ve formátu `<device name>\<user alias>` (např. `DESKTOP-123\John.Smith`).
- **Název počítače** – `%COMPUTER_NAME%`.

  Název počítače, na kterém bylo zablokováno spuštění souboru.
- **Název spustitelného souboru** – `%FILE_NAME%`.

  Název spustitelného souboru zablokované aplikace.
- **Kategorie KL spustitelného souboru** – `%KL_CAT%`.

  Kategorie KL, do které zablokovaná aplikace patří (například *Prohlížeče* nebo jiná kategorie).
- **Cesta ke spustitelnému souboru** – `%FILE_PATH%`.

  Úplná cesta ke spustitelnému souboru procesu zablokované aplikace.
- **Verze spustitelného souboru** – `%FILE_VERSION%`.

  Verze spustitelného souboru zablokované aplikace.
- **Původní název spustitelného souboru** – `%ORIGINAL_FILE_NAME%`.

  Původní název spustitelného souboru zablokované aplikace. Název souboru je zadán ve vlastnostech spustitelného souboru aplikace.
- **Dodavatel** – `%FILE_PUBLISHER%`.

Dodavatel zablokované aplikace.

- **Název aplikace** – `%FILE_PRODUCT_NAME%`.

  Název zablokované aplikace.

- **Verze aplikace** – `%PRODUCT_VERSION%`.

  Verze zablokované aplikace.

- **Hash spustitelného souboru** – `%FILE_HASH%`.

  Hodnota hash spustitelného souboru zablokované aplikace.

- **Vystavitel certifikátu** – `%CERT_ISSUER%`.

  Vydavatel certifikátu, kterým je spustitelný soubor podepsán.

- **Předmět certifikátu** – `%CERT_SUBJECT%`.

  Předmět certifikátu, kterým je spustitelný soubor podepsán.

- **Kryptografický otisk certifikátu** – `%CERT_THUMBPRINT%`.

  Miniatura certifikátu, kterým je spustitelný soubor podepsán.

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:

   - **Category with content added manually**. 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.

     - Složka aplikace. 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.

- **Category that includes executable files from a specific folder**. Můžete určit složku, ze které budou spustitelné soubory automaticky přiřazeny k vytvořené kategorii aplikací.
- **Category that includes executable files from selected devices**. 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 **Executable files**.

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.

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 **Subject** 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, Ochrana před webovými hrozbami, Detekce chování a Prevence zneužití 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.

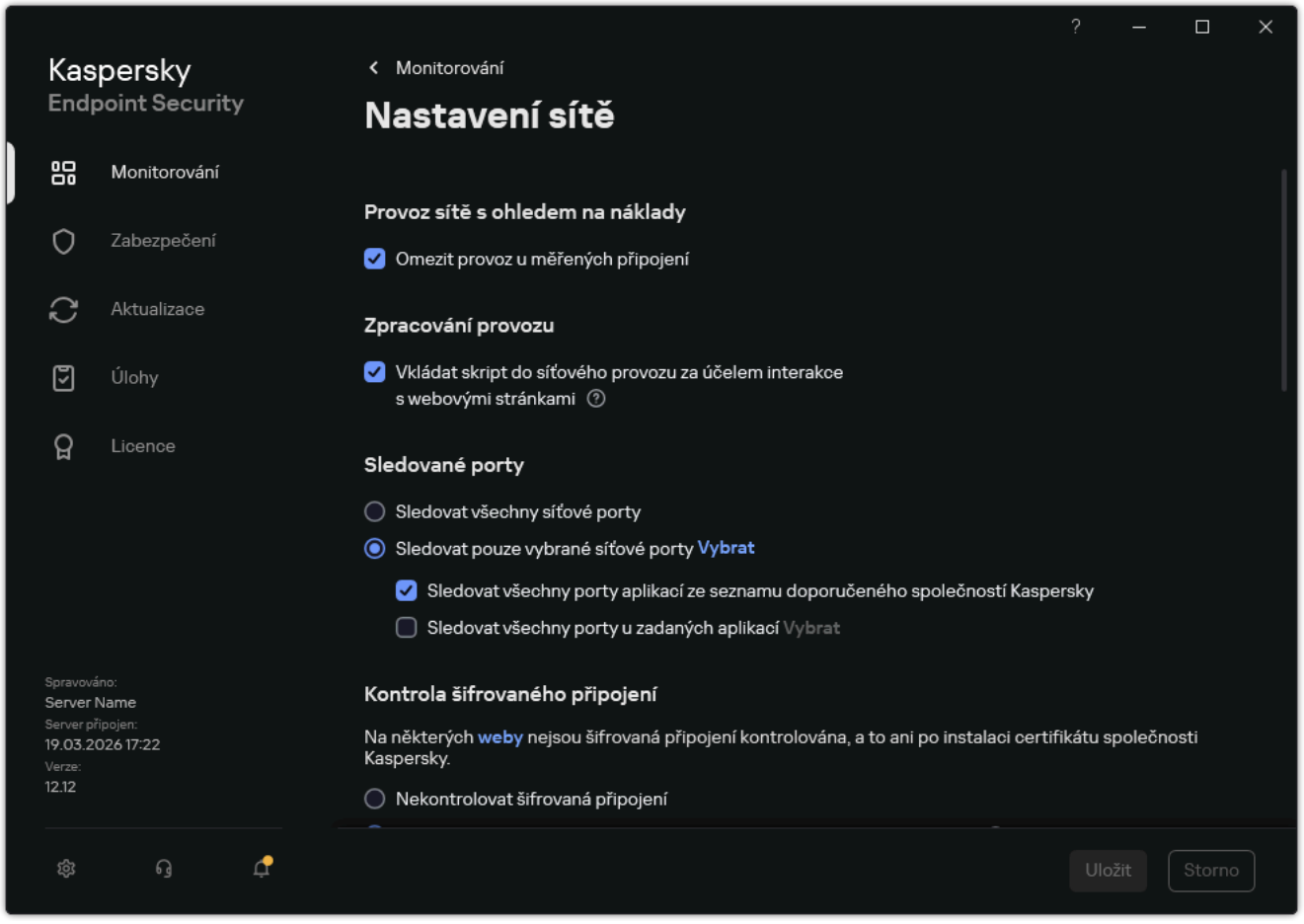
Aplikace Kaspersky Endpoint Security dělí porty TCP a UDP počítače uživatele do několika skupin v závislosti na pravděpodobnosti jejich zneužití. Některé síťové porty jsou vyhrazeny pro zranitelné služby. Doporučujeme sledovat tyto porty důkladněji, protože je u nich větší pravděpodobnost, že na ně bude 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.

Aby byla zajištěna bezpečnost počítače, součásti Detekce chování a Prevence zneužití také monitorují datové toky procházející síťovými porty. Tyto součásti průběžně monitorují síťový provoz a vyhledávají v něm jednotlivé procesy, které mohou být ohrožující.

Povolení monitorování všech síťových portů

Postup povolení monitorování všech síťových portů:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.



Nastavení sledování síťových portů

3. V bloku **Sledované porty** vyberte položku **Sledovat všechny síťové porty**.

4. Uložte změny.

Vytvoření seznamu sledovaných síťových portů

Změnu seznamu monitorovaných síťových portů mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Postup vytvoření seznamu sledovaných síťových portů:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.

3. V bloku **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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení sítě**.

3. V bloku **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 Acrobat 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. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Network Settings**.
5. Postup exportu seznamu síťových portů:
   a. V bloku **Monitored ports** vyberte položku **Monitor selected network ports only**.
   b. Klikněte na odkaz **selected N ports**.
      Otevře se okno **Network ports**. V okně **Network ports** 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 **Export**.
   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. Uložte soubor.

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 **Monitored ports** zaškrtněte políčko **Monitor all ports for specified applications**.

   b. Klikněte na odkaz **selected N applications**.

   c. V seznamu aplikací vyberte aplikace, které chcete exportovat.

   d. Klikněte na tlačítko **Export**.

   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. Uložte soubor.

   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 **Import**.

   V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam síťových portů.

   b. Otevřete soubor.

   Pokud počítač již seznam síťových portů obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

8. Postup importu seznamu aplikací, jejichž porty jsou monitorovány aplikací Kaspersky Endpoint Security:

   a. V seznamu aplikací klikněte na tlačítko **Import**.

   V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam aplikací.

   b. Otevřete soubor.

   Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

9. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Nastavení sítě**.

4. V bloku **Sledované porty** vyberte položku **Sledovat pouze vybrané síťové porty**.

5. 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.

6. 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. Uložte soubor.

   Aplikace Kaspersky Endpoint Security exportuje celý seznam síťových portů do souboru XML.

7. 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. Uložte soubor.

Aplikace Kaspersky Endpoint Security exportuje celý seznam aplikací do souboru XML.

8. 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. Otevřete soubor.

Pokud počítač již seznam síťových portů obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

9. 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. Otevřete soubor.

Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

10. Uložte změny.

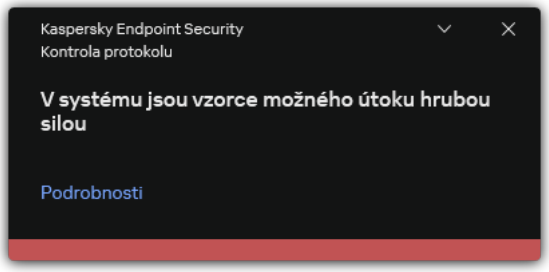
Kontrola protokolu

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice.

Od verze 11.11.0 zahrnuje aplikace Kaspersky Endpoint Security pro systém Windows součást Kontrola protokolu. Kontrola protokolu monitoruje integritu chráněného prostředí na základě analýzy protokolu událostí systému Windows. Pokud aplikace zjistí známky netypického chování systému, informuje o tom správce, protože toto chování může znamenat pokus o kybernetický útok.

Kaspersky Endpoint Security analyzuje protokoly událostí systému Windows a v souladu s pravidly zjišťuje porušení. Součást zahrnuje předdefinovaná pravidla. Předdefinovaná pravidla jsou založena na heuristické analýze. Můžete také přidat vlastní pravidla (vlastní pravidla). Když se pravidlo spustí, aplikace vytvoří událost se stavem *Critical* (viz obrázek níže).

Pokud chcete používat součást Kontrola protokolu, ujistěte se, že je nakonfigurováno nastavení zabezpečení zásad auditu a že systém zaznamenává do protokolu příslušné události (podrobnosti najdete na webu technické podpory společnosti Microsoft).



Upozornění součásti Kontrola protokolu

Konfigurace předdefinovaných pravidel

Předdefinovaná pravidla zahrnují šablony abnormální aktivity v chráněném počítači. Abnormální aktivita může znamenat pokus o útok. Předdefinovaná pravidla jsou založena na heuristické analýze. Pro součást Kontrola protokolu je k dispozici sedm předdefinovaných pravidel. Kterékoli z těchto pravidel můžete povolit nebo zakázat. Předdefinovaná pravidla nelze odstranit.

Můžete nakonfigurovat kritéria spouštění pro pravidla, která monitorují události, u následujících operací:

- Detekce hesla hrubou silou
- Detekce přihlášení k síti

Jak konfigurovat předdefinovaná pravidla v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola protokolu**.
4. Ujistěte se, že je zaškrtnuto políčko **Kontrola protokolu**.
5. V bloku **Předdefinovaná pravidla** klikněte na tlačítko **Nastavení**.
6. Zaškrtnutím nebo zrušením zaškrtnutí políček nakonfigurujte předdefinovaná pravidla:
   - **V systému jsou vzorce možného útoku hrubou silou**.
   - **Během relace přihlášení k síti byla zjištěna atypická aktivita**.
   - **Jsou přítomny vzorce možného zneužití protokolu událostí systému Windows**.
   - **Byly zjištěny atypické akce prováděné pro novou nainstalovanou službu**.
   - **Bylo zjištěno atypické přihlášení, které používá explicitní přihlašovací údaje**.
   - **V systému jsou vzorce možného útoku prostřednictvím zfalšovaného certifikátu PAC protokolu Kerberos (MS14-068)**.
   - **Byly zjištěny podezřelé změny v integrované skupině s oprávněními Správci**.
7. V případě potřeby nakonfigurujte pravidlo **V systému jsou vzorce možného útoku hrubou silou**:
   a. Klikněte na tlačítko **Nastavení** pod příslušným pravidlem.
   b. V okně, které se otevře, zadejte počet pokusů a časové období, během kterého musí být provedeny pokusy o zadání hesla, aby se pravidlo aktivovalo.
   c. Klikněte na tlačítko **OK**.
8. Pokud jste vybrali pravidlo **Během relace přihlášení k síti byla zjištěna atypická aktivita**, musíte nakonfigurovat jeho nastavení:
   a. Klikněte na tlačítko **Nastavení** pod příslušným pravidlem.
   b. V bloku **Detekce přihlášení k síti** zadejte počátek a koncem časového intervalu.
      Kaspersky Endpoint Security považuje pokusy o přihlášení provedené během zadaného intervalu jako abnormální aktivitu.
      Ve výchozím nastavení není interval nastaven a aplikace nesleduje pokusy o přihlášení. Aby aplikace nepřetržitě monitorovala pokusy o přihlášení, nastavte interval na 00:00–23:59. Začátek a konec intervalu se nesmí shodovat. Pokud jsou stejné, aplikace nesleduje pokusy o přihlášení.
   c. Vytvořte seznam důvěryhodných uživatelů a důvěryhodných IP adres (IPv4 a IPv6).
      Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Kaspersky Endpoint Security nemonitoruje pokusy o přihlášení u těchto uživatelů a počítačů.
   d. Klikněte na tlačítko **OK**.
9. Uložte změny.

Jak konfigurovat předdefinovaná pravidla ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls → Log Inspection**.

5. Ujistěte se, že je zapnut přepínač **Log Inspection ENABLED**.

6. V bloku **Predefined rules** povolte nebo zakažte předdefinovaná pravidla pomocí přepínačů:

   - **There are patterns of a possible brute-force attack in the system**.
   - **There is an atypical activity detected during a network logon session**.
   - **There are patterns of a possible Windows Event Log abuse**.
   - **Atypical actions detected on behalf of a new service installed**.
   - **Atypical logon that uses explicit credentials detected**.
   - **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

   a. **Suspicious changes detected in the privileged built-in Administrators group**.

7. V případě potřeby nakonfigurujte pravidlo **There are patterns of a possible brute-force attack in the system**:

   a. Klikněte na **Settings** pod příslušným pravidlem.

   b. V okně, které se otevře, zadejte počet pokusů a časové období, během kterého musí být provedeny pokusy o zadání hesla, aby se pravidlo aktivovalo.

   c. Klikněte na tlačítko **OK**.

8. Pokud jste vybrali pravidlo **There is an atypical activity detected during a network logon session**, musíte nakonfigurovat jeho nastavení:

   a. Klikněte na **Settings** pod příslušným pravidlem.

   b. V bloku **Network logon detection** zadejte počátek a koncem časového intervalu.

   Kaspersky Endpoint Security považuje pokusy o přihlášení provedené během zadaného intervalu jako abnormální aktivitu.

   Ve výchozím nastavení není interval nastaven a aplikace nesleduje pokusy o přihlášení. Aby aplikace nepřetržitě monitorovala pokusy o přihlášení, nastavte interval na 00:00–23:59. Začátek a konec intervalu se nesmí shodovat. Pokud jsou stejné, aplikace nesleduje pokusy o přihlášení.

   c. V bloku **Exclusions** přidejte důvěryhodné uživatele a důvěryhodné IP adresy (IPv4 a IPv6).

   Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Kaspersky Endpoint Security nemonitoruje pokusy o přihlášení u těchto uživatelů a počítačů.

   d. Klikněte na tlačítko **OK**.

9. Uložte změny.

Jak konfigurovat předdefinovaná pravidla v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Kontrola protokolu**.

3. Ujistěte se, že je zapnut přepínač **Kontrola protokolu**.

4. V bloku **Předdefinovaná pravidla** klikněte na tlačítko **Konfigurovat**.

5. Zaškrtnutím nebo zrušením zaškrtnutí políček nakonfigurujte předdefinovaná pravidla:

   - **V systému jsou vzorce možného útoku hrubou silou**.
   - **Během relace přihlášení k síti byla zjištěna atypická aktivita**.
   - **Jsou přítomny vzorce možného zneužití protokolu událostí systému Windows**.
   - **Byly zjištěny atypické akce prováděné pro novou nainstalovanou službu**.
   - **Bylo zjištěno atypické přihlášení, které používá explicitní přihlašovací údaje**.

- **V systému jsou vzorce možného útoku prostřednictvím zfalšovaného certifikátu PAC protokolu Kerberos (MS14-068)**.

a. **Byly zjištěny podezřelé změny v integrované skupině s oprávněními Správci**.

6. V případě potřeby nakonfigurujte pravidlo **V systému jsou vzorce možného útoku hrubou silou**:

a. Klikněte na **Nastavení** pod příslušným pravidlem.

b. V okně, které se otevře, zadejte počet pokusů a časové období, během kterého musí být provedeny pokusy o zadání hesla, aby se pravidlo aktivovalo.

7. Pokud jste vybrali pravidlo **Během relace přihlášení k síti byla zjištěna atypická aktivita**, musíte nakonfigurovat jeho nastavení:

a. Klikněte na **Nastavení** pod příslušným pravidlem.

b. V bloku **Detekce přihlášení k síti** zadejte počátek a koncem časového intervalu.

Kaspersky Endpoint Security považuje pokusy o přihlášení provedené během zadaného intervalu jako abnormální aktivitu.

Ve výchozím nastavení není interval nastaven a aplikace nesleduje pokusy o přihlášení. Aby aplikace nepřetržitě monitorovala pokusy o přihlášení, nastavte interval na 00:00–23:59. Začátek a konec intervalu se nesmí shodovat. Pokud jsou stejné, aplikace nesleduje pokusy o přihlášení.

c. V bloku **Výjimky** přidejte důvěryhodné uživatele a důvěryhodné IP adresy (IPv4 a IPv6).

Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Kaspersky Endpoint Security nemonitoruje pokusy o přihlášení u těchto uživatelů a počítačů.

8. Uložte změny.

Výsledkem je, že při spuštění pravidla vytvoří aplikace Kaspersky Endpoint Security událost *Kritická událost*.

Přidávání vlastních pravidel

Můžete si nastavit vlastní kritéria pro aktivaci pravidel součásti Kontrola protokolu. K tomu musíte zadat ID události a vybrat zdroj události. ID události si můžete vyhledat na webu technické podpory společnosti Microsoft. Zdroj událostí můžete vybrat ze standardních protokolů: *Application*, *Security* nebo *System*. Můžete rovněž zadat protokol aplikace třetí strany. Název protokolu aplikace třetí strany zjistíte pomocí nástroje Prohlížeč událostí. Protokoly aplikace třetí strany jsou uchovávány ve složce Protokoly aplikací a služeb (například protokol *Windows PowerShell*).

Aplikace nekontroluje, zda je zadaný protokol skutečně přítomen v protokolu událostí systému Windows. Pokud je v názvu protokolu chyba, aplikace události z tohoto protokolu nesleduje.

Seznam vlastních pravidel již obsahuje tři pravidla vytvořená odborníky společnosti Kaspersky.

Jak přidat vlastní pravidlo v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Kontrola protokolu**.
4. Ujistěte se, že je zaškrtnuto políčko **Kontrola protokolu**.
5. V bloku **Vlastní pravidla** klikněte na tlačítko **Nastavení**.
6. V okně, které se otevře, zaškrtněte políčka vedle vlastních pravidel, která chcete povolit.
7. V případě nutnosti klikněte na tlačítko **Přidat** a vyberte vlastní pravidla.
8. Otevře se okno, ve kterém nakonfigurujte vlastní pravidlo:

- **Název pravidla**.
- **Název protokolu**. Protokoly událostí systému Windows. K dispozici jsou následující protokoly: *Application*, *Security*, *System*.
- **Zdroj**. Protokoly aplikací třetích stran. Název protokolu aplikace třetí strany zjistíte pomocí nástroje Prohlížeč událostí. Protokoly aplikace třetí strany jsou uchovávány ve složce Protokoly aplikací a služeb (například protokol *Windows PowerShell*).
- **Identifikátory událostí**. ID událostí v protokolu událostí systému Windows. ID události si můžete vyhledat v technické dokumentaci společnosti Microsoft.

9. Uložte změny.

Jak přidat vlastní pravidlo ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **Log Inspection**.
5. Ujistěte se, že je zapnut přepínač **Log Inspection ENABLED**.
6. V bloku **Custom rules** vyberte vlastní pravidla, která chcete upravit.
7. V případě nutnosti klikněte na tlačítko **Add** a vyberte vlastní pravidla.
8. Otevře se okno, ve kterém nakonfigurujte vlastní pravidlo:
   - **Rule name**.
   - **Custom log name**. Protokoly událostí systému Windows. K dispozici jsou následující protokoly: *Application*, *Security*, *System*.
   - **Origin**. Protokoly aplikací třetích stran. Název protokolu aplikace třetí strany zjistíte pomocí nástroje Prohlížeč událostí. Protokoly aplikace třetí strany jsou uchovávány ve složce Protokoly aplikací a služeb (například protokol *Windows PowerShell*).
   - **Event Identifiers**. ID událostí v protokolu událostí systému Windows. ID události si můžete vyhledat v technické dokumentaci společnosti Microsoft.
9. Uložte změny.

Jak přidat vlastní pravidlo v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Kontrola protokolu**.
3. Ujistěte se, že je zapnut přepínač **Kontrola protokolu**.
4. V bloku **Vlastní pravidla** klikněte na tlačítko **Konfigurovat**.
5. V okně, které se otevře, zaškrtněte políčka vedle vlastních pravidel, která chcete povolit.
6. V případě nutnosti klikněte na tlačítko **Přidat** a vyberte vlastní pravidla.
7. Otevře se okno, ve kterém nakonfigurujte vlastní pravidlo:
   - **Název pravidla**.
   - **Název protokolu**. Protokoly událostí systému Windows. K dispozici jsou následující protokoly: *Application*, *Security*, *System*.
   - **Zdroj**. Protokoly aplikací třetích stran. Název protokolu aplikace třetí strany zjistíte pomocí nástroje Prohlížeč událostí. Protokoly aplikace třetí strany jsou uchovávány ve složce Protokoly aplikací a služeb (například protokol *Windows PowerShell*).
   - **Identifikátor události**. ID událostí v protokolu událostí systému Windows. ID události si můžete vyhledat v technické dokumentaci společnosti Microsoft.
8. Uložte změny.

Výsledkem je, že při spuštění pravidla vytvoří aplikace Kaspersky Endpoint Security událost *Critical*.

Monitorování integrity systému

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice.

Od verze 12.6 obsahuje aplikace Kaspersky Endpoint Security pro systém Windows místo součásti Monitor integrity souborů součást Monitorování integrity systému. Součást Monitorování integrity systému zahrnuje veškeré funkce součásti Monitor integrity souborů a navíc umožňuje sledovat změny registru a připojení externích zařízení.

Součást Monitorování integrity systému monitoruje změny v operačním systému, které mohou naznačovat narušení zabezpečení počítače. V případě zjištění takovýchto změn Kaspersky Endpoint Security vygeneruje odpovídající události a upozorní správce. Monitorování integrity systému může fungovat v reálném čase a může také provádět kontroly integrity systému na vyžádání.

Monitorování integrity systému v reálném čase

V režimu monitorování v reálném čase Monitorování integrity systému sleduje změny v objektech, které jste zahrnuli do rozsahu součásti (*rozsah monitorování*). Monitorování integrity systému také umožňuje blokovat neoprávněný přístup k takovým objektům v reálném čase.

Kontrola integrity systému na vyžádání

Kontrola integrity systému na vyžádání je úloha, kterou můžete spustit ručně nebo podle plánu. Chcete-li úlohu *Kontrola integrity systému* spustit, musíte nakonfigurovat rozsah součásti (*rozsah sledování*) a vytvořit základní stav. *Základní stav* je zaznamenaný stav objektů v systému, který aplikace používá jako referenci při porovnávání s aktuálním stavem.

Migrace nastavení funkce Monitor integrity souborů

Když aktualizujete aplikaci Kaspersky Endpoint Security na verzi 12.6, nastavení součásti Monitor integrity souborů se migrují automaticky. V rámci migrace aplikace přesune pravidla monitorování do součásti Monitorování integrity systému. Pravidla součásti Monitor integrity souborů jsou také migrována do součásti Monitorování integrity systému, když migrujete z KSWS na KES.

Pro zajištění správného fungování součásti Monitorování integrity systému je třeba aktualizovat aplikaci Kaspersky Endpoint Security i modul plug-in administrace na verzi 12.6. Pokud máte nainstalovanou starší verzi modulu plug-in pro správu, nemůžete konfigurovat monitorování integrity systému, protože v modulu plug-in pro správu není část **Monitorování integrity systému**.

O pravidlech součásti Monitorování integrity systému

Aby součást Monitorování integrity systému fungovala, musíte přidat alespoň jedno pravidlo. *Pravidlo součásti Monitorování integrity systému* je sada kritérií, která definují přístup uživatelů k souborům a registru. Monitorování integrity systému zjišťuje změny v souborech a registru v rámci zadaného *rozsahu monitorování*. Rozsah monitorování je jedním z kritérií pravidla součásti Monitorování integrity systému.

Monitorování integrity systému umožňuje monitorování následujících objektů:

- Soubory
- Registr
- Externí zařízení

Zvláštní úvahy spojené s monitorováním souborů

Monitorování integrity systému monitoruje změny souborů a složek a také soubory přidávané do rozsahu monitorování nebo z něj odstraňované. Tyto změny mohou znamenat narušení zabezpečení počítače. Doporučujeme přidávat zřídka měněné objekty nebo objekty, ke kterým má přístup pouze správce. Tím se sníží počet událostí součásti Monitorování integrity systému.

Monitorování integrity systému nemonitoruje změny souborů ve sdílených složkách serveru. Monitorování integrity systému lze používat pouze místně.

Kaspersky Endpoint Security monitoruje změny souborů a složek pouze na těch discích, které byly připojeny, když bylo spuštěno monitorování integrity systému v reálném čase. Pokud disk nebyl připojen, když začalo monitorování integrity systému v reálném čase, aplikace nesleduje změny souborů a složek na tomto disku, i když jsou soubory a složky přidány do rozsahu monitorování.

Zvláštní úvahy spojené s monitorováním registru

Sledování integrity systému monitoruje registr. Tyto změny mohou znamenat narušení zabezpečení počítače.

Monitorování integrity systému monitoruje následující kořenové klíče registru:

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG (k dispozici pouze v součásti Monitorování integrity systému v reálném čase)
- HKEY_CURRENT_USER (k dispozici pouze v součásti Monitorování integrity systému v reálném čase)

  Úloha *Kontrola integrity systému* nepodporuje klíč HKEY_CURRENT_USER. Můžete zadat klíč pod HKEY_USERS jako HKEY_USERS\<user profile ID>\<key>.

Zvláštní úvahy spojené s monitorováním externích zařízení

Monitorování integrity systému monitoruje připojení a odpojení externích zařízení. To je nezbytné pro ochranu počítače před bezpečnostními hrozbami, které mohou vyplynout z výměny souborů s takovými zařízeními. Monitorování integrity systému nesleduje přístup k externím zařízením a neblokuje výměnu souborů. Můžete nakonfigurovat přístup k zařízením pomocí jiné součásti aplikace, Kontrola zařízení.

Při spuštění úlohy *Monitor integrity systému v porovnání se základním stavem* bude aplikace ignorovat opětovné připojování externích zařízení, pokud mají zařízení v operačním systému stejné písmeno jednotky. Aby mohla být znovu připojená zařízení zaznamenána, musí mít jiná písmena jednotek.

Monitorování integrity systému monitoruje připojení následujících typů externích zařízení:

- Vyměnitelná jednotka (včetně USB flash disků)
- Pevný disk
- Externí síťový adaptér
- Disk CD/DVD/Blu-ray
- Skener/fotoaparát

Monitorování integrity systému v reálném čase

Monitorování integrity systému umožňuje sledovat změny v operačním systému v reálném čase. Můžete sledovat změny, které mohou naznačovat narušení zabezpečení počítače. Tato součást umožňuje blokování těchto změn nebo pouze protokolování změnových událostí.

Aby součást Monitorování integrity systému fungovala, musíte přidat alespoň jeden pravidlo. *Pravidlo součásti Monitorování integrity systému* je sada kritérií, která definují přístup uživatelů k souborům a registru. Monitorování integrity systému zjišťuje změny v souborech a registru v rámci zadaného *rozsahu monitorování*. Rozsah monitorování je jedním z kritérií pravidla součásti Monitorování integrity systému.

Režimy součásti Monitorování integrity systému v reálném čase

Chcete-li zajistit, aby pravidla součásti Monitorování integrity systému neblokovala žádné akce se zdroji, které jsou kritické pro fungování operačního systému nebo jiných služeb, doporučujeme povolit testovací režim a analyzovat, jak tato součásti ovlivňuje systém. Při zapnutém testovacím režimu Kaspersky Endpoint Security neblokuje aktivitu uživatele, která je zakázána pravidly, ale generuje události *Varování* ⚠.

Součást Monitorování integrity systému v reálném čase má dva režimy:

- Blokovat

  V tomto režimu součást Monitorování integrity systému monitoruje změny v systému a provádí akci v souladu s pravidly: **Povolit** nebo **Blokovat**. Monitorování integrity systému také vygeneruje odpovídající událost a změní stav zařízení v konzole aplikace Kaspersky Security Center.

- Informovat

  V tomto režimu umožňuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování. Pokud je akce se soubory nebo registrem zakázána, aplikace vygeneruje událost: *Zakázaná operace byla povolena v testovacím režimu*. Chcete-li analyzovat, jak pravidla ovlivňují systém, můžete se podívat na zprávy.

Povolení součásti Monitorování integrity systému v reálném čase

Jak povolit součást Monitorování integrity systému v reálném čase v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Monitorování integrity systému**.
4. Zaškrtněte políčko **Monitorování integrity systému**.
5. V části **Režim fungování pro pravidla blokování** vyberte režim součásti Monitorování integrity systému v reálném čase:
   - **Blokovat**. V tomto režimu blokuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.
   - **Informovat**. V tomto režimu umožňuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.
6. V bloku **Monitorování integrity systému v reálném čase** zaškrtněte políčko **Monitorování integrity systému v reálném čase**.
7. Konfigurace monitorování externích zařízení:
   a. Zaškrtněte políčko **Monitorovat zařízení**.
   b. V rozevíracím seznamu **Závažnost události** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informační*, *Varování*, *Kritická*.

   Součást Monitorování integrity systému zaznamenává aktuální připojení externích zařízení. Aplikace začne sledovat připojení a odpojení externích zařízení poté, co je tato součást povolena v nastavení aplikace. Následně, když je externí zařízení připojeno nebo odpojeno, aplikace vygeneruje odpovídající událost.
8. Konfigurace monitorování souborů a registru:
   a. Zaškrtněte políčko **Monitorovat soubory a registr**.
   b. Klikněte na tlačítko **Nastavení**.
      Otevře se seznam pravidel součásti Monitorování integrity systému.
   c. Klikněte na tlačítko **Přidat**.
      Můžete také importovat pravidla z jiného zdroje.
   d. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).
9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit součást Monitorování integrity systému v reálném čase ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **System Integrity Monitoring**.
5. Zapněte přepínač **System Integrity Monitoring ENABLED**.
6. Vyberte kartu **Windows**.
7. V části **Real-Time System Integrity Monitoring** vyberte režim součásti Monitorování integrity systému v reálném čase:
   - **Apply rules**. V tomto režimu blokuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.

- **Test rules (Inform)**. V tomto režimu umožňuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.

8. Konfigurace monitorování souborů a registru:

   a. Zaškrtněte políčko **Monitor files and the registry**.

   b. Klikněte na tlačítko **Rules**.

   Otevře se seznam pravidel součásti Monitorování integrity systému.

   c. Klikněte na tlačítko **Add**.

   Můžete také importovat pravidla z jiného zdroje.

   d. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).

9. Konfigurace monitorování externích zařízení:

   a. Zaškrtněte políčko **Monitor devices**.

   b. V rozevíracím seznamu **Event severity level** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informational*, *Warning*, *Critical*.

Součást Monitorování integrity systému zaznamenává aktuální připojení externích zařízení. Aplikace začne sledovat připojení a odpojení externích zařízení poté, co je tato součást povolena v nastavení aplikace. Následně, když je externí zařízení připojeno nebo odpojeno, aplikace vygeneruje odpovídající událost.

10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit součást Monitorování integrity systému v reálném čase v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení → Monitorování integrity systému**.

3. Zapněte přepínač **Monitorování integrity systému**.

4. V části **Režim fungování pro pravidla blokování** vyberte režim součásti Monitorování integrity systému v reálném čase:

   - **Blokovat**. V tomto režimu blokuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.

   - **Informovat**. V tomto režimu umožňuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.

5. V bloku **Monitorování integrity systému v reálném čase** zaškrtněte políčko **Monitorování integrity systému v reálném čase**.

6. Konfigurace monitorování externích zařízení:

   a. Zaškrtněte políčko **Monitorovat zařízení**.

   b. V rozevíracím seznamu **Závažnost události** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informační*, *Varování*, *Kritická*.

Součást Monitorování integrity systému zaznamenává aktuální připojení externích zařízení. Aplikace začne sledovat připojení a odpojení externích zařízení poté, co je tato součást povolena v nastavení aplikace. Následně, když je externí zařízení připojeno nebo odpojeno, aplikace vygeneruje odpovídající událost.

7. Konfigurace monitorování souborů a registru:

   a. Zaškrtněte políčko **Monitorovat soubory a registr**.

   b. Klikněte na tlačítko **Nastavit**.

   Otevře se seznam pravidel součásti Monitorování integrity systému.

   c. Klikněte na tlačítko **Přidat**.

   Můžete také importovat pravidla z jiného zdroje.

8. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).

9. Uložte změny.

Nastavení pravidel součásti Monitorování integrity systému v reálném čase

Parametr	Popis
Název pravidla	Název pravidla součásti Monitorování integrity systému v reálném čase
Operace se soubory a registrem	• **Povolit**. Součást Monitorování integrity systému umožňuje akce se soubory a klíči registru z rozsahu monitorování. • **Blokovat**. Chování součásti Monitorování integrity systému závisí na zvoleném režimu. Pokud jste vybrali *Režim ochrany systému*, součást Monitorování integrity systému blokuje akce se soubory a klíči registru z rozsahu monitorování, vygeneruje odpovídající událost a změní stav zařízení v konzole Kaspersky Security Center. Pokud jste vybrali *Režim testování*, součást Monitorování integrity systému umožňuje akce se soubory a klíči registru z rozsahu monitorování.
Závažnost události	Kaspersky Endpoint Security zaznamenává do protokolu události změn souboru, kdykoli dojde ke změně souboru nebo klíče registru v rozsahu monitorování. K dispozici jsou následující závažnosti událostí: *Informační*, *Varování*, *Kritická*.
Rozsah monitorování	• **Soubor**. Seznam souborů a složek sledovaných součástí. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků. • **Registr**. Seznam klíčů registru a hodnot sledovaných součástí. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.
Výjimky	• **Soubor**. Seznam výjimek z rozsahu monitorování. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Například `C:\Folder\Application\*.log`. Položky výjimek mají vyšší prioritu než položky rozsahu monitorování. 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků. • **Registr**. Seznam výjimek z rozsahu monitorování. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`. Položky výjimek mají vyšší prioritu než položky rozsahu monitorování.
Důvěryhodní uživatelé a/nebo skupiny uživatelů	*Důvěryhodný uživatel* je uživatel, který má povoleno provádět akce se soubory a klíči registru v rozsahu monitorování. Pokud aplikace Kaspersky Endpoint Security zjistí akci provedenou důvěryhodným uživatelem, součást Monitorování integrity systému vygeneruje *Informační* událost. Můžete vybrat uživatele v Active Directory, v seznamu účtů v aplikaci Kaspersky Security Center nebo ručním zadáním místního uživatelského jména. Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty.
Deskriptory operace se souborem / Monitorované operace	Značky charakterizující akci se soubory nebo klíči registru, které bude aplikace monitorovat.

Hashování	Výpočet hodnoty hash souboru při úpravě. Kaspersky Endpoint Security přidává informace o hodnotě hash souboru, když je vygenerována událost.

Kontrola integrity systému na vyžádání

Kontrola integrity systému na vyžádání je úloha, kterou můžete spustit ručně nebo podle plánu. Při spuštění úlohy *Kontrola integrity systému* aplikace porovnává aktuální stav objektů zařazených do rozsahu monitorování s jejich *základním stavem*. Na rozdíl od monitorování integrity systému v reálném čase úloha *Kontrola integrity systému* pomáhá omezit počet událostí a umožňuje generovat celkovou zprávu o změnách v operačním systému.

Aby součást Monitorování integrity systému fungovala, musíte přidat alespoň jeden pravidlo. *Pravidlo součásti Monitorování integrity systému* je sada kritérií, která definují přístup uživatelů k souborům a registru. Monitorování integrity systému zjišťuje změny v souborech a registru v rámci zadaného *rozsahu monitorování*. Rozsah monitorování je jedním z kritérií pravidla součásti Monitorování integrity systému. Můžete nakonfigurovat pravidla pro sdílení pomocí součásti Monitorování integrity systému v reálném čase a úlohu *Kontrola integrity systému* nebo vytvořit pro úlohu samostatná pravidla. K vytvoření základního stavu uplatní aplikace Kaspersky Endpoint Security rozsah monitorování z úlohy *Kontrola integrity systému* na úlohu *Aktualizace základního stavu*.

Vytvoření a aktualizace základního stavu

Aby mohla úloha *Kontrola integrity systému* fungovat, potřebuje základní stav. *Základní stav* je zaznamenaný stav objektů v systému, který aplikace používá jako referenci při porovnávání s aktuálním stavem. Pokud se aktuální stav systému liší od stavu systému zaznamenaného v základním stavu, aplikace Kaspersky Endpoint Security vygeneruje odpovídající událost. Základní stav můžete vytvořit nebo aktualizovat pomocí úlohy *Aktualizace základního stavu*.

Základní stav můžete aktualizovat v následujících režimech:

- Úplná aktualizace.

  Aplikace aktualizuje všechny objekty v rozsahu monitorování.

- Inkrementální aktualizace.

  Aplikace detekuje a aktualizuje pouze upravené nebo nové objekty.

Jak vytvořit nebo aktualizovat základní stav v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Aktualizace základního stavu**.

Krok 2. Výběr režimu aktualizace základního stavu

Vyberte režim aktualizace základního stavu:

- **Úplná aktualizace**. Aplikace aktualizuje všechny objekty v rozsahu monitorování.
- **Inkrementální aktualizace**. Aplikace detekuje a aktualizuje pouze upravené nebo nové objekty.

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 *Základní stav 2024*.

Krok 5. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak vytvořit nebo aktualizovat základní stav ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **Baseline update**.
   c. Do pole **Task name** zadejte krátký popis, například *Základní stav 2024*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Klikněte na novou úlohu.
   Otevře se okno vlastností úlohy.
8. Vyberte kartu **Application settings**.
9. Vyberte režim aktualizace základního stavu:
   - **Full update**. Aplikace aktualizuje všechny objekty v rozsahu monitorování.
   - **Incremental update**. Aplikace detekuje a aktualizuje pouze upravené nebo nové objekty.
10. Uložte změny.
11. Zaškrtněte políčko vedle úlohy.
12. Klikněte na tlačítko **Start**.

Konfigurace rozsahu monitorování pro úlohu Kontrola integrity systému

Ve výchozím nastavení je rozsah monitorování úlohy *Kontrola integrity systému* stejný jako rozsah monitorování součásti Monitorování integrity systému v reálném čase. Pro úlohu můžete nakonfigurovat jiný rozsah monitorování.

Monitorování integrity systému nepodporuje import klíčů `HKEY_CURRENT_USER` a `HKEY_CURRENT_CONFIG` u úlohy *Kontrola integrity systému*. Pokud rozsah monitorování úlohy obsahuje tyto klíče, aplikace vygeneruje událost *Součástí monitorování jsou nesprávné objekty*.

Jak nakonfigurovat jiný rozsah monitorování pro úlohu Kontrola integrity systému v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Monitorování integrity systému**.

4. Zaškrtněte políčko **Monitorování integrity systému**.

5. V části **Kontrola integrity systému** vyberte režim konfigurace úlohy: **Konfigurovat pravidla**.

6. Konfigurace monitorování externích zařízení:

   a. Zaškrtněte políčko **Monitorovat zařízení**.

   b. V rozevíracím seznamu **Závažnost události** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informační*, *Varování*, *Kritická*.

   Monitorování integrity systému zaznamenává informace o připojených externích zařízeních v době, kdy je vytvořen základní stav. Následně, když je připojeno externí zařízení, aplikace vygeneruje odpovídající událost. Při spuštění úlohy *Kontrola integrity systému* aplikace nesleduje odpojení externích zařízení.

7. Konfigurace monitorování souborů a registru:

   a. Zaškrtněte políčko **Monitorovat soubory a registr**.

   b. Klikněte na tlačítko **Nastavení**.

   Otevře se seznam pravidel součásti Monitorování integrity systému.

   c. Klikněte na tlačítko **Přidat**.

   Můžete také importovat pravidla z jiného zdroje.

   d. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).

8. Uložte změny.

Jak nakonfigurovat jiný rozsah monitorování pro úlohu System Integrity Check úkolu ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Security Controls** → **System Integrity Monitoring**.

5. Vyberte kartu **Windows**.

6. Zapněte přepínač **System Integrity Monitoring ENABLED**.

7. V části **System Integrity Check** vyberte režim konfigurace úlohy: **Custom settings**.

8. Konfigurace monitorování externích zařízení:

   a. Zaškrtněte políčko **Monitor devices**.

   b. V rozevíracím seznamu **Event severity level** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informational*, *Warning*, *Critical*.

   Monitorování integrity systému zaznamenává informace o připojených externích zařízeních v době, kdy je vytvořen základní stav. Následně, když je připojeno externí zařízení, aplikace vygeneruje odpovídající událost. Při spuštění úlohy *Kontrola integrity systému* aplikace nesleduje odpojení externích zařízení.

9. Konfigurace monitorování souborů a registru:

   a. Zaškrtněte políčko **Monitor files and the registry**.

   b. Klikněte na tlačítko **Rules**.

   Otevře se seznam pravidel součásti Monitorování integrity systému.

   c. Klikněte na tlačítko **Add**.

   Můžete také importovat pravidla z jiného zdroje.

   d. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).

10. Uložte změny.

Jak nakonfigurovat jiný rozsah monitorování pro úlohu Kontrola integrity systému v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Kontrolní prvky zabezpečení** → **Monitorování integrity systému**.
3. Zapněte přepínač **Monitorování integrity systému**.
4. V části **Kontrola integrity systému** vyberte režim konfigurace úlohy: **Vlastní nastavení**.
5. Konfigurace monitorování externích zařízení:
   a. Zaškrtněte políčko **Monitorovat zařízení**.
   b. V rozevíracím seznamu **Závažnost události** vyberte úroveň důležitosti událostí monitorování externích zařízení: *Informační*, *Varování*, *Kritická*.

   Monitorování integrity systému zaznamenává informace o připojených externích zařízeních v době, kdy je vytvořen základní stav. Následně, když je připojeno externí zařízení, aplikace vygeneruje odpovídající událost. Při spuštění úlohy *Kontrola integrity systému* aplikace nesleduje odpojení externích zařízení.
6. Konfigurace monitorování souborů a registru:
   a. Zaškrtněte políčko **Monitorovat soubory a registr**.
   b. Klikněte na tlačítko **Nastavit**.
      Otevře se seznam pravidel součásti Monitorování integrity systému.
   c. Klikněte na tlačítko **Přidat**.
      Můžete také importovat pravidla z jiného zdroje.
   d. Nakonfigurujte pravidlo součásti Monitorování integrity systému (viz tabulka níže).
7. Uložte změny.

Nastavení pravidla úlohy Kontrola integrity systému

Parametr	Popis
Název pravidla	Název pravidla úlohy *Kontrola integrity systému*.
Závažnost události	Kaspersky Endpoint Security zaznamenává do protokolu události změn souboru, kdykoli dojde ke změně souboru nebo klíče registru v rozsahu monitorování. K dispozici jsou následující závažnosti událostí: *Informační*, *Varování*, *Kritická*.
Rozsah monitorování	• **Soubor**. Seznam souborů a složek sledovaných součástí. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků. • **Registr**. Seznam klíčů registru a hodnot sledovaných součástí. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.
Výjimky	• **Soubor**. Seznam výjimek z rozsahu monitorování. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Například `C:\Folder\Application\*.log`. Položky výjimek mají vyšší prioritu než položky rozsahu monitorování.

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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

- **Registr**. Seznam výjimek z rozsahu monitorování. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`. Položky výjimek mají vyšší prioritu než položky rozsahu monitorování.

Spuštění úlohy Kontrola integrity systému

Úloha *Kontrola integrity systému* umožňuje kontrolu změn souborů nebo klíčů registru a také kontrolu připojení externích zařízení. Chcete-li zkontrolovat změny souborů, můžete spustit úlohu *Kontrola integrity systému* v následujících režimech:

- Rychlá kontrola.

  Při kontrole souborů na změny aplikace kontroluje pouze atributy souborů. Nekontroluje obsah souborů.

- Úplná kontrola,

  Při kontrole souborů na změny aplikace kontroluje všechny atributy souborů a obsah souborů.

Režim, ve kterém je úloha spuštěna, neovlivňuje kontrolu registru ani externích zařízení.

Jak spustit úlohu Kontrola integrity systému v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.

   Otevře se seznam úloh.
3. Klikněte na tlačítko **New task**.

   Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.
4. Vyberte možnost **Kaspersky Endpoint Security → Monitor integrity systému v porovnání se základním stavem**. Vyberte režim Monitorování integrity systému:
   - **Úplná kontrola**. V tomto režimu aplikace kontroluje všechny atributy a hodnoty hash souborů.
   - **Rychlá kontrola**. V tomto režimu aplikace kontroluje pouze atributy souborů.
5. Vyberte počítače, na kterých bude úloha provedena. K dispozici jsou následující možnosti:
   - 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.
   - Určete výběr zařízení, na kterých chcete úlohu spouštět.
   - Přiřaďte úlohu ke skupině pro správu. V tomto případě je úloha přiřazena k počítačům zahrnutým v dříve vytvořené skupině pro správu.
6. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
7. Nakonfigurujte plán pro spuštění úlohy, například ručně nebo v konkrétní den týdne.
8. Zadejte název úlohy.
9. Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak spustit úlohu System Integrity Check ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **System Integrity Check**.
   c. Do pole **Task name** zadejte krátký popis, například *Týdenní kontrola integrity systému*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Klikněte na novou úlohu.
   Otevře se okno vlastností úlohy.
8. Vyberte kartu **Application settings**.
9. Vyberte režim Kontrola integrity systému:
   - **Quick Scan**. Aplikace kontroluje pouze atributy souborů. Nekontroluje obsah souborů.
   - **Full Scan**. Aplikace kontroluje všechny atributy souborů i jejich obsah.
10. Uložte změny.
11. Zaškrtněte políčko vedle úlohy.
12. Klikněte na tlačítko **Start**.

Aby byla úloha *Kontrola integrity systému* úspěšně dokončena, rozsah monitorování úlohy *Kontrola integrity systému* se musí zcela shodovat se základním stavem. Pokud je rozsah monitorování jiný, úloha skončí s chybou. Chcete-li synchronizovat rozsahy monitorování, spusťte úlohu *Aktualizace základního stavu* s novým rozsahem monitorování.

Export a import pravidel součásti Monitorování integrity systému

Seznam pravidel součásti Monitorování integrity systému můžete exportovat do souboru XML. Pak můžete soubor upravit, například přidat velké množství záznamů stejného typu. Můžete použít funkci exportu/importu k zálohování seznamu pravidel součásti Monitorování integrity systému nebo k migraci seznamu na jiný server.

Monitorování integrity systému nepodporuje import klíčů `HKEY_CURRENT_USER` a `HKEY_CURRENT_CONFIG` u úlohy *Kontrola integrity systému*. Pokud rozsah monitorování úlohy obsahuje tyto klíče, aplikace vygeneruje událost *Součástí monitorování jsou nesprávné objekty*.

Jak exportovat a importovat seznam pravidel součásti Monitorování integrity systému v reálném čase v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Kontrolní prvky zabezpečení** → **Monitorování integrity systému**.

4. Postup exportu nebo importu pravidel součásti *Monitorování integrity systému v reálném čase*:

   a. V bloku **Monitorování integrity systému v reálném čase** klikněte na tlačítko **Nastavení**.

   b. Postup exportu seznamu pravidel součásti Monitorování integrity systému v reálném čase:

      1. 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.

      2. Klikněte na odkaz **Exportovat**.

      3. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.

      4. Uložte soubor.

         Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.

   c. Postup importu seznamu pravidel součásti Monitorování integrity systému v reálném čase:

      1. Klikněte na odkaz **Importovat**.

         V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.

      2. Otevřete soubor.

         Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

5. Postup exportu nebo importu pravidel součásti *Kontrola integrity systému*:

   a. V bloku **Kontrola integrity systému** vyberte položku **Konfigurovat pravidla**.

   b. Klikněte na tlačítko **Nastavení**.

   c. Postup exportu seznamu pravidel součásti Kontrola integrity systému:

      1. 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.

      2. Klikněte na odkaz **Exportovat**.

      3. V okně, které se otevře, zadejte název souboru XML, do kterého chcete exportovat seznam pravidel, a vyberte složku, do které chcete tento soubor uložit.

      4. Uložte soubor.

      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.

   d. Postup importu seznamu pravidel součásti Kontrola integrity systému:

      1. Klikněte na odkaz **Importovat**.

         V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.

      2. Otevřete soubor.

      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

6. Uložte změny.

[Jak exportovat a importovat seznam pravidel součásti Monitorování integrity systému ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Security Controls** → **System Integrity Monitoring**.

5. Vyberte kartu **Windows**.

6. Postup exportu nebo importu pravidel součásti *Monitorování integrity systému v reálném čase*:

   a. V bloku **Real-Time System Integrity Monitoring** klikněte na odkaz **Rules**.

   b. Postup exportu seznamu pravidel součásti Monitorování integrity systému v reálném čase:

      1. Vyberte pravidla, která chcete exportovat.

      2. Klikněte na tlačítko → **Export**.
         Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru JSON ve výchozí složce pro stahování.

   c. Postup importu seznamu pravidel součásti Monitorování integrity systému v reálném čase:

      1. Klikněte na tlačítko → **Import**.
         V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam důvěryhodných adres.

      2. Otevřete soubor.
         Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.

7. Postup exportu nebo importu pravidel součásti *Kontrola integrity systému*:

   a. V bloku **On-Demand System Integrity Check** vyberte položku **Custom settings**.

   b. Klikněte na odkaz **Rules**.

   c. Postup exportu seznamu pravidel součásti Kontrola integrity systému:

      1. Vyberte pravidla, která chcete exportovat.

      2. Klikněte na tlačítko → **Export**.
         Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru JSON ve výchozí složce pro stahování.

   d. Postup importu seznamu pravidel součásti Kontrola integrity systému:

      1. Klikněte na tlačítko → **Import**.
         V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam důvěryhodných adres.

      2. Otevřete soubor.
         Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.

8. Uložte změny.

Zobrazení zpráv součásti Monitorování integrity systému

Chcete-li analyzovat výkon pravidel součásti Monitorování integrity systému, můžete se podívat na zprávy a události generované aplikací. Kaspersky Endpoint Security generuje následující zprávy týkající se součásti:

- V rozhraní aplikace:
  - Zpráva součásti Monitorování integrity systému
  - Zpráva součásti Kontrola integrity systému
  - Zpráva o aktualizaci základního stavu

  Zprávy obsahují události součásti Monitorování integrity systému.
- V konzole aplikace Kaspersky Security Center:
  - Zpráva o počítačích, na kterých byla pravidla monitorování aktivována nejvícekrát
  - Zpráva o nejčastěji aktivovaných pravidlech monitorování

  Ve výchozím nastavení je zpráva vytvářena za předchozích 30 dní, včetně data jejího vytvoření.

[Jak zobrazit zprávy Monitorování integrity systému v konzole pro správu (MMC)]

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 New Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V kroku **Selecting the report template type** vyberte zprávu Monitorování integrity systému (část **Other**):
   - **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   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.

[Jak zobrazit zprávy Monitorování integrity systému ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Monitoring** → **Reports**.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce New Report Template Wizard.
3. V části **Template type**, v **Other** vyberte zprávu Monitorování integrity systému:
   - **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
   - **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

   Jakmile budete s průvodcem New Report Template Wizard hotovi, zobrazí se nová šablona zprávy v tabulce.
4. Vyberte a spusťte zprávu.

Spustí se proces generování zprávy. Zpráva se zobrazí v novém okně.

Chcete-li zobrazit události generované aplikací, můžete také použít výběr událostí v konzole aplikace Kaspersky Security Center.

Obnovení stavu integrity systému

Počítače v konzole aplikace Kaspersky Security Center mají jeden z následujících stavů: *OK*, *Warning* nebo *Critical*. Pokud součást Monitorování integrity systému zjistí úpravu souborů nebo klíčů registru v rozsahu monitorování, stav počítače se změní na *Warning* nebo *Critical*. Stav přiřazený součástí Monitorování integrity systému se nazývá *stav integrity systému*. Stav integrity systému můžete resetovat, například pokud vás analýza přesvědčí, že zjištěná úprava objektů nemá vliv na zabezpečení počítače.

[Jak resetovat stav integrity systému v konzole pro správu (MMC)]

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Obnovení stavu integrity systému**.

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 úloh, například ručně.

Krok 4. Definování názvu úlohy

Zadejte název úlohy, např. *Resetování stavu po úpravě rozsahu monitorování*.

Krok 5. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak resetovat stav integrity systému ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.
   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:
   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.
   b. V rozevíracím seznamu **Task type** vyberte možnost **System integrity status reset**.
   c. Do pole **Task name** zadejte stručný popis, např. *Resetování stavu po úpravě rozsahu monitorování*.
   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte účet pro spuštění úlohy. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spustí úlohu s oprávněními místního uživatelského účtu.
6. Ukončete průvodce.
   V seznamu úloh se zobrazí nová úloha.
7. Zaškrtněte políčko vedle úlohy.
8. Klikněte na tlačítko **Start**.

Výsledkem je, že pokud byl stav počítače změněn na *Warning* nebo *Critical* kvůli událostem součásti Monitorování integrity systému, je stav počítače resetován na *OK*. Pokud se stav počítače změnil také kvůli jiným událostem, jeho stav zůstane nezměněn.

Cloud Discovery

Cloud Discovery spravuje přístup uživatelů ke cloudovým službám. Mezi cloudové služby patří například Microsoft Teams, Salesforce nebo Microsoft Office 365. Cloudové služby jsou seskupeny do kategorií, například *Sdílení souborů*, *Messengery* nebo *E-mail*. Odborníci společnosti Kaspersky pravidelně kategorie Cloud Discovery a služby do nich zařazené aktualizují. Aplikace Kaspersky Endpoint Security aktualizuje sadu kategorií a cloudových služeb spolu s databázemi aplikací. To znamená, že Cloud Discovery pro kategorizaci cloudových služeb nepoužívá službu Kaspersky Security Network.

Cloud Discovery poskytuje následující služby:

- Monitorování používání cloudových služeb

- Blokování přístupu uživatelů ke cloudovým službám

Požadavky na systém

Cloud Discovery je k dispozici, pokud jsou splněny níže uvedené podmínky:

- Aplikace je nainstalována na počítači se systémem Windows pro pracovní stanice.

  Součást není k dispozici pro servery.

- Kaspersky Security Center verze 15.1 nebo novější.

  Součást není k dispozici v konzole pro správu (MMC). Cloud Discovery můžete konfigurovat ve webové konzole aplikace Kaspersky Security Center a cloudové konzole aplikace Kaspersky Security Center.

- Licence Kaspersky Next.

Povolte funkce aplikace, které součást Cloud Discovery vyžaduje:

1. **Kontrola šifrovaného připojení**. Tato funkce je nutná pro monitorování provozu HTTPS. Spravovat ji můžete v části **Nastavení sítě**.
2. **Vkládat skript do síťového provozu za účelem interakce s webovými stránkami**. Skript umožňuje registraci událostí Cloud Discovery. Skript také umožňuje plnohodnotné blokování přístupu ke cloudovým službám. Bez skriptu aplikace blokuje přístup pouze doménám cloudových služeb. Spravovat ji můžete v části **Nastavení sítě**.

Můžete také povolit funkci **Protokolovat otvírání povolených stránek**. Součástí této funkce je seskupování událostí, když uživatel navštíví webové stránky, které patří do stejné domény. Když uživatel používá cloudovou službu, Cloud Discovery tak do protokolu zaznamená pouze jednu událost, nikoli více událostí pro každou webovou stránku. Spravovat ji můžete v části **Kontrola webu**.

Monitorování cloudových služeb

Když uživatel začne používat cloudovou službu, aplikace Kaspersky Endpoint Security tuto událost zaregistruje a vytvoří záznam ve zprávě. Cloud Discovery kontroluje používání cloudových služeb v prohlížeči a odpovídajících aplikacích. Cloud Discovery kontroluje používání cloudových služeb přes HTTP a HTTPS.

[Jak povolit monitorování cloudových služeb v cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection** → **Cloud Discovery**.
5. Zapněte přepínač **Cloud Discovery ENABLED**.
6. Uložte změny.

Aplikace tak předává informace o používaných cloudových službách do aplikace Kaspersky Security Center. Informace o používání cloudových služeb si můžete prohlédnout ve zprávách. V případě potřeby můžete zablokovat přístup ke cloudovým službám.

Blokování přístupu ke cloudovým službám

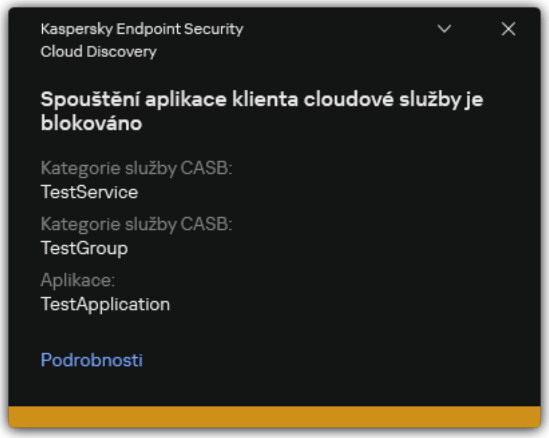
Blokování přístup ke cloudovým službám je k dispozici pouze u licence Kaspersky Next EDR Optimum a XDR Expert. Tato funkce není dostupná pro licenci Kaspersky Next EDR Foundations. Porovnání funkčnosti aplikace v závislosti na typu licence Kaspersky Next najdete v nápovědě k aplikaci Kaspersky Next.

Správce může uživatelům omezit přístup ke kategoriím Cloud Discovery nebo jednotlivým cloudovým službám. Může tak povolit pouze bezpečné cloudové služby a předcházet tak únikům dat. U každé cloudové služby se ve funkci Cloud Discovery zobrazují *informace o úrovni rizika*. Úroveň rizika pomáhá odhalit služby, které nesplňují bezpečnostní požadavky organizace.

Úroveň rizika je odhad a neznamená žádné prohlášení o kvalitě cloudové služby či jejího dodavatele. Úroveň rizika je pouze doporučením odborníků společnosti Kaspersky.

Úrovně rizika cloudových služeb se zobrazují v části **Cloud Discovery** příslušné zásady v seznamu všech kontrolovaných cloudových služeb.

Další součásti aplikace Kaspersky Endpoint Security poskytují ochranu před hrozbami a sledování podezřelých aktivit uživatelů při používání cloudových služeb.



Upozornění funkce Cloud Discovery

Cloud Discovery neblokuje cloudové aplikace spuštěné před aplikací Kaspersky Endpoint Security.

Jak blokovat přístup ke cloudovým službám v cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Communication & Web Protection** → **Cloud Discovery**.
5. Zapněte přepínač **Cloud Discovery ENABLED**.
   Zobrazí se seznam všech cloudových služeb. Cloudové služby jsou seskupeny do kategorií, například *File sharing*, *Messengers*, *Email*. Odborníci společnosti Kaspersky pravidelně kategorie Cloud Discovery a služby do nich zařazené aktualizují. Aplikace Kaspersky Endpoint Security aktualizuje sadu kategorií a cloudových služeb spolu s databázemi aplikací.
6. Nakonfigurujte přístup ke cloudovým službám pomocí přepínače **Access**.
7. Uložte změny.

Aplikace tak kontroluje používání cloudových služeb v prohlížeči a odpovídajících aplikacích.

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.

U aplikace Kaspersky Endpoint Security pro systém Windows můžete od verze 12.5 přidávat telemetrii EDR do důvěryhodné zóny. To umožňuje optimalizovat data, která aplikace odesílá na server pro shromažďování telemetrie u řešení Kaspersky Anti Targeted Attack Platform (EDR).

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware.

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 mohou útočníci využívat k poškození počítače nebo osobních dat, najdete na webu 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.
- Úloha *Kontrola malwaru*.

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.

Změnu seznamu výjimek z kontroly mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak vytvořit výjimku z kontroly v konzole pro správu (MMC)

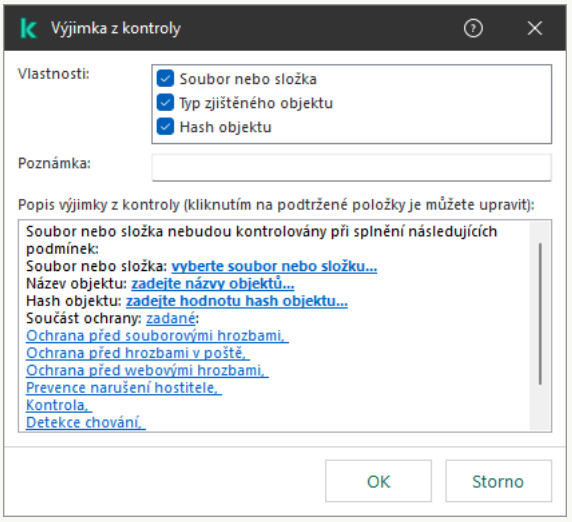
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
4. V bloku **Výjimky z kontroly a důvěryhodné aplikace** → **Výjimky z kontroly** klikněte na tlačítko **Nastavení**.

   Otevře se okno obsahující seznam výjimek z kontroly.
5. 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.
6. Pokud chcete uživateli umožnit vytvoření místního seznamu důvěryhodných aplikací, 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam výjimek z kontroly v uživatelském rozhraní aplikace.
7. Klikněte na tlačítko **Přidat** a vyberte akci:

- **Kategorie**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
- **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
- **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.
- **Nová výjimka ve vybrané kategorii**. Chcete-li přidat novou výjimku z kontroly do konkrétní kategorie, vyberte kategorii.

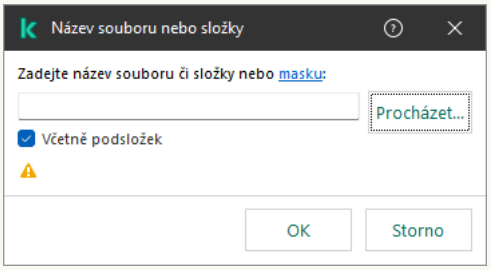
8. Postup vyloučení souboru nebo složky z kontroly:



Nastavení výjimek

a. V bloku **Vlastnosti** zaškrtněte políčko **Soubor nebo složka**.

b. Kliknutím na odkaz v bloku níže otevřete okno **Název souboru nebo složky**.



Vybrat soubor nebo složku

a. 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

Kaspersky Endpoint Security podporuje proměnné prostředí

Síťové složky můžete vyloučit. To provedete tak, že ručně zadáte cestu k síťové složce (např. `\\Network Share\*`).

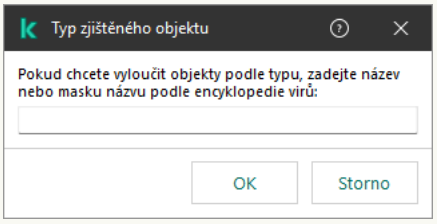
Kaspersky Endpoint Security nepodporuje při generování seznamu výjimek z kontroly v konzole aplikace Kaspersky Security Center proměnnou prostředí `%userprofile%`. chcete-li položku použít na všechny uživatelské účty, můžete použít znak `*` (například `C:\Users\*\Documents\File.exe`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

b. Uložte změny.

9. Postup vyloučení objektů určitého názvu z kontroly:

a. V bloku **Vlastnosti** zaškrtněte políčko **Typ zjištěného objektu**.

b. Kliknutím na odkaz v bloku níže otevřete okno **Typ zjištěného objektu**.



Vybrat objekt

a. 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`.

b. Uložte změny.

10. Pokud chcete z kontroly vyloučit jednotlivý soubor:

a. V bloku **Vlastnosti** zaškrtněte políčko **Hash objektu**.

b. Kliknutím na odkaz v bloku níže otevřete okno **Hash objektu**.



Výběr souboru

a. Zadejte hodnotu hash souboru nebo vyberte požadovaný soubor po kliknutí na tlačítko **Procházet**.

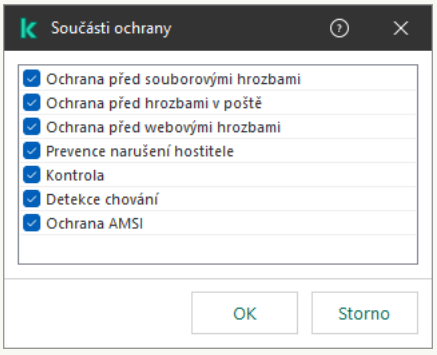
V případě změny soubory se změní také hodnota hash souboru. V tomto případě nebude upravený soubor přidán k výjimkám.

b. Uložte změny.

11. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

12. Určete, které součásti aplikace Kaspersky Endpoint Security mají výjimku z kontroly použít:

a. Kliknutím na odkaz v bloku níže otevřete okno **Součásti ochrany**.



Vybrat součásti ochrany

a. Zaškrtněte políčka vedle součástí, u kterých se má výjimka z kontroly použít.

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.

13. Klikněte na tlačítko **OK**.

Nová výjimka bude přidána do seznamu. Výjimku můžete kdykoli zakázat pomocí zaškrtávacího políčka vedle příslušného objektu.

14. Uložte změny.

[Jak vytvořit výjimku z kontroly ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.
4. Přejděte do části **Trusted Zone**.
5. V okně, které se otevře, klikněte na odkaz **Malware Scan exclusions**.
6. Pokud chcete vytvořit konsolidovaný seznam výjimek z kontroly pro všechny počítače ve společnosti, zaškrtněte políčko **Merge values when inheriting**. 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 důvěryhodných aplikací, zaškrtněte políčko **Allow use of local exclusions**. 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam výjimek z kontroly v uživatelském rozhraní aplikace.

8. Klikněte na tlačítko **Add** a vyberte akci:

- **Category**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
- **New exclusion**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
- **Select exclusion from list**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.

Chcete-li přidat novou výjimku z kontroly do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **New exclusion**.

9. Vyberte, jak chcete výjimku přidat: **Path to the file or folder**, **Object type** nebo **Object hash**.
10. Chcete-li vyloučit z kontroly soubor nebo složku, zadejte cestu ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

Síťové složky můžete vyloučit. To provedete tak, že ručně zadáte cestu k síťové složce (např. `\\Network Share\*`).

11. Chcete-li z kontroly vyloučit určitý typ objektu, zadejte do pole **Object type** 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 **Object hash** 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 **Apply exclusion to** vyberte součásti, pro které chcete výjimky z kontroly použít.

14. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Comment**.

15. Klikněte na tlačítko **OK**.

    Nová výjimka bude přidána do seznamu. Pomocí přepínače můžete výjimku kdykoli ukončit.

16. Uložte změny.

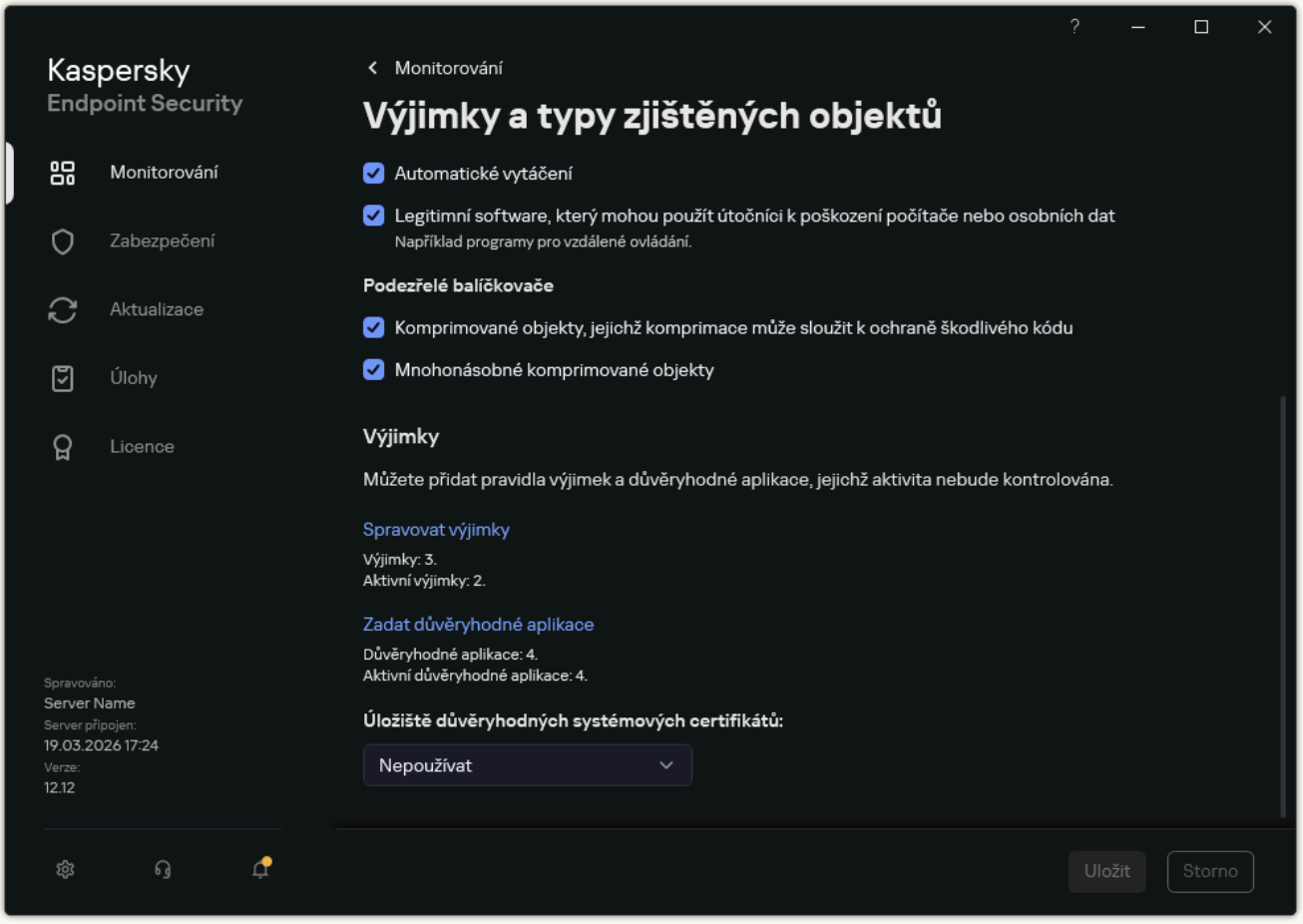
Jak vytvořit výjimku z kontroly v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Výjimky a typy zjištěných objektů**.

3. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.

   Kaspersky Endpoint Security skryje seznam výjimek z kontroly v uživatelském rozhraní aplikace, pokud je konfigurace výjimek z kontroly blokována správcem v konzole (symbol „zavřeného zámku“) a místní výjimky z kontroly jsou zakázány (není zaškrtnuto políčko **Povolit používání místních výjimek**).



Nastavení výjimek

4. Klikněte na tlačítko **Přidat** a vyberte akci:

- **Kategorie**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
- **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
- **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.

Chcete-li přidat novou výjimku z kontroly do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **Nová výjimka**.

5. Pokud chcete z kontroly vyloučit soubor nebo složku, vyberte je po kliknutí na tlačítko **Procházet**.

   Cestu můžete rovněž zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

     Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

     Síťové složky můžete vyloučit. To provedete tak, že ručně zadáte cestu k síťové složce (např. `\\Network Share\*`).

6. Chcete-li z kontroly vyloučit určitý typ objektu, zadejte do pole **Typ zjištěného objektu** 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`.

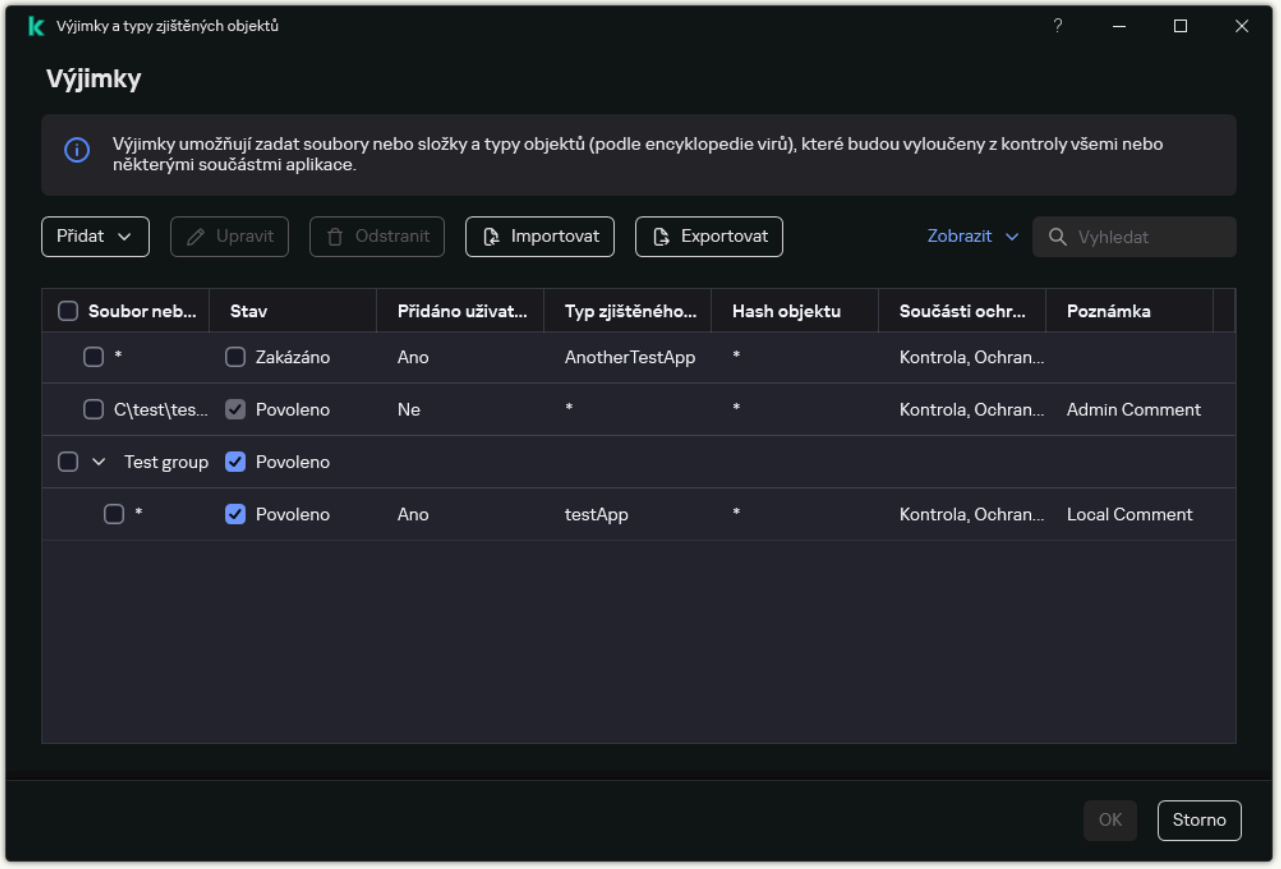
7. Chcete-li z kontroly vyloučit jednotlivý soubor, do pole **Hash objektu** zadejte hodnotu hash tohoto souboru.

   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**.
11. Klikněte na tlačítko **Přidat**.

    Nová výjimka bude přidána do seznamu. Výjimku můžete kdykoli zakázat pomocí zaškrtávacího políčka vedle sloupce **Stav**.

12. Uložte změny.



Seznam výjimek

Příklady masky cesty:

Místo absolutních cest doporučujeme zadávat relativní cesty. To umožňuje vyloučit nejen objekty systému souborů, ale také objekty bez souborů. Například `*\Program Files (x86)\Folder\Subfolder`.

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\`, včetně podložek.
- Maska `C:\dir\` bude představovat všechny cesty k souborům umístěným ve složce `C:\dir\`, včetně podložek.
- 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\`.
- Maska `C:\dir1\*\dir3\` bude zahrnovat všechny cesty k souborům v podsložkách dir3 jednu úroveň do složky `C:\dir1\`.
- Maska `C:\dir1\**\dirN\` bude zahrnovat všechny cesty k souborům v podsložkách dirN ve složce `C:\dir1\` na jakékoli úrovni.

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.

Vytvoření výjimky podle typu zjištěných objektů

Aplikace Kaspersky Endpoint Security klasifikuje zjištěné objekty následujícím způsobem:

- Viry a červy

  Podkategorie: Viry a červy (Viruses_and_Worms)

  Úroveň nebezpečí: 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. *Overwriting* viry přepíší svůj kód přes kód infikovaného souboru, čímž se obsah souboru vymaže. Infikovaný soubor přestane fungovat a nebude možné jej obnovit. *Parasitic* viry upravují soubory a zanechají se plně nebo částečně funkční. *Companion* 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: *Link viry*, *viry OBJ*, *viry LIB*, viry *zdrojového kódu* a mnoho dalších.

  Worm

  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.
IM-Worm	Červi klienta 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.
IRC-Worm	Červi internetových konverzací	Šíří se prostřednictvím 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.
Net-Worm	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.

P2P-Worm	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.
Worm	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 (včetně ransomwaru)

Podkategorie: Trojské koně

Úroveň nebezpečí: 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.
Backdoor	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.
Trojan	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 „útočníkovi" 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

Constructor	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 nebezpečí: 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: Automatické vytáčení (Dialer).

  Úroveň nebezpečí: Střední

Automatické vytáčení může tajně navázat telefonní spojení pomocí modemu.

- Legitimní software, který mohou použít útočníci k poškození počítače nebo osobních dat

  Podkategorie: legitimní software, který mohou útočníci použít 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.
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

  Podkategorie: Zabalené soubory, které mohou způsobit škodu.

  Úroveň nebezpečí: střední.

  Soubor je zabalen pomocí speciálního komprimačního programu, který se používá pro balení malwaru: virů, červů, trojských koní. Aplikace Kaspersky Endpoint Security kontroluje rozbalovací modul v (samorozbalovacích) archivech SFX.

Aby hackeři skryli malware před detekcí antivirem, zabalí jej pomocí speciálních komprimačních programů. Odborníci společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

- Mnohonásobné komprimované objekty

  Podkategorie: mnohonásobně komprimované soubory.

  Úroveň nebezpečí: střední.

  Soubor je třikrát nebo vícekrát sbalen jedním nebo více komprimačními programy.

  Aby hackeři skryli malware před detekcí antivirem, mohou soubor zabalit několikrát. Aplikace Kaspersky Endpoint Security kontroluje zabalené soubory.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security zjišťuje všechny typy objektů. Pro zvýšení zabezpečení počítače doporučujeme ponechat povolenou detekci všech typů objektů. Pokud používáte interní nástroje, které aplikace zjistí jako škodlivé, přidejte tyto nástroje na seznam výjimek, ale nezakazujte detekci celého typu objektů.

Jak vybrat typy zjišťovaných objektů v konzole pro správu (MMC)

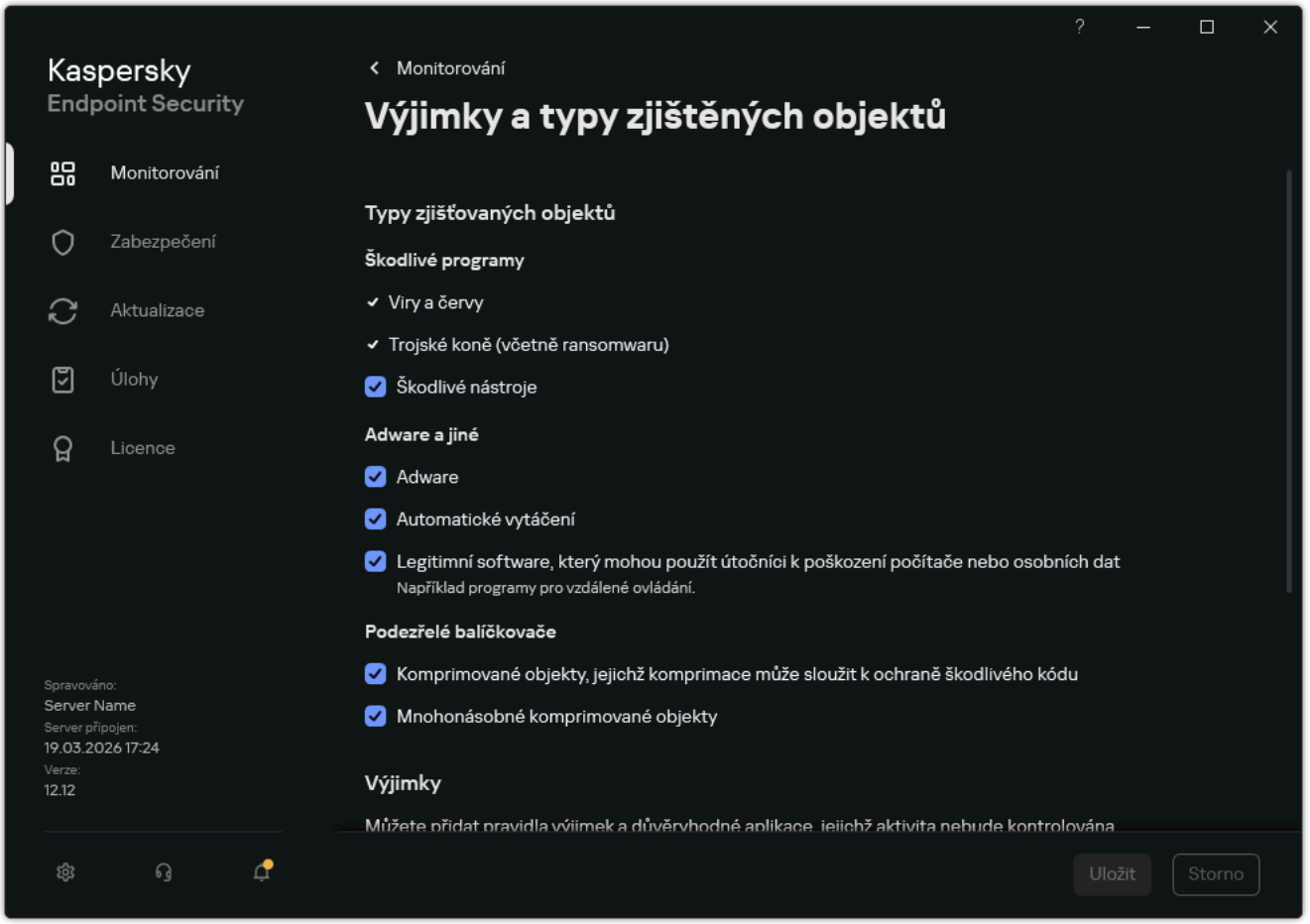
1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
5. V bloku **Typy zjišťovaných objektů** klikněte na tlačítko **Nastavení**.
6. V okně, které se otevře, zaškrtněte políčka u typů objektů, které má aplikace Kaspersky Endpoint Security zjišťovat.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak vybrat typy zjišťovatelných objektů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Detection Settings**.
5. V bloku **Detection of other types of objects** zaškrtněte políčka u typů objektů, které má aplikace Kaspersky Endpoint Security zjišťovat.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak vybrat typy zjišťovaných objektů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.
3. V bloku **Typy zjišťovaných objektů** zaškrtněte políčka u typů objektů, které má aplikace Kaspersky Endpoint Security zjišťovat.
4. Uložte změny.



Typy zjišťovaných objektů

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 monitoruje objekty, které jsou otevírané, spouštěné nebo ukládané jakýmkoli procesem aplikace, a kontroluje činnost všech aplikací a veškerý síťový provoz, který tyto aplikace vygenerují. Po přidání aplikace do seznamu důvěryhodných aplikací přestane aplikace Kaspersky Endpoint Security monitorovat činnost této aplikace.

Rozdíl mezi výjimkami z kontroly a důvěryhodnými aplikacemi je v tom, že u výjimky aplikace Kaspersky Endpoint Security nekontroluje soubory, zatímco u důvěryhodných aplikací nekontroluje spouštěné procesy. Pokud důvěryhodná aplikace vytvoří škodlivý soubor ve složce, která není zahrnuta ve výjimkách z kontroly, aplikace Kaspersky Endpoint Security tento soubor detekuje a hrozbu odstraní. Jestliže je složka přidána do výjimek, Kaspersky Endpoint Security tento soubor přeskočí.

Pokud například považujete objekty používané standardní aplikací Poznámkový blok v systému Microsoft Windows za bezpečnou (tj. této aplikaci důvěřujete), může ji přidat na seznam důvěryhodných aplikací, aby objekty používané touto aplikací nebyly sledovány. To zvýší výkon počítače, což je zvláště důležité při používání serverových aplikací.

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.

Důvěryhodné aplikace pomáhají předcházet problémům s kompatibilitou mezi aplikací Kaspersky Endpoint Security a jinými aplikacemi (například problém dvojité kontroly síťového provozu počítače třetí strany aplikací Kaspersky Endpoint Security a jinou antivirovou 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.

Změnu seznamu důvěryhodných aplikací mohou blokovat vlastnosti nadřazené zásady. Chcete-li seznam změnit, musíte povolit změnu nastavení důvěryhodné zóny ve webové konzole („visací zámek" musí být odemčený).

Důvěryhodné zóny jsou v konzole pro správu (MMC) a ve webové konzole seskupeny odlišně. Stejně tak se liší způsob zamezení změnám parametru důvěryhodné zóny (různé „visací zámky"). Pro správu aplikace doporučujeme používat pouze webovou konzolu. Pokud nakonfigurujete důvěryhodnou zónu v různých konzolách, může modul plug-in pro správu resetovat „visací zámek" do výchozího stavu.

Jak přidat aplikaci na seznam důvěryhodných v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.

4. V bloku **Výjimky z kontroly a důvěryhodné aplikace** → **Důvěryhodné aplikace** klikněte na tlačítko **Nastavení**.

   Otevře se okno obsahující seznam důvěryhodných aplikací.

5. 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.

6. 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam důvěryhodných aplikací v uživatelském rozhraní aplikace.

7. Klikněte na tlačítko **Přidat** a vyberte akci:

   - **Kategorie**. Důvěryhodné aplikace můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu důvěryhodnou aplikaci.
   - **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou důvěryhodnou aplikaci do kořenového seznamu.
   - **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované důvěryhodné aplikace*. Byly také přidány důvěryhodné aplikace z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované důvěryhodné aplikace.
   - **Nová výjimka ve vybrané kategorii**. Chcete-li přidat novou důvěryhodnou aplikaci do určité kategorie, vyberte kategorii.

8. Vyberte kritéria důvěry:

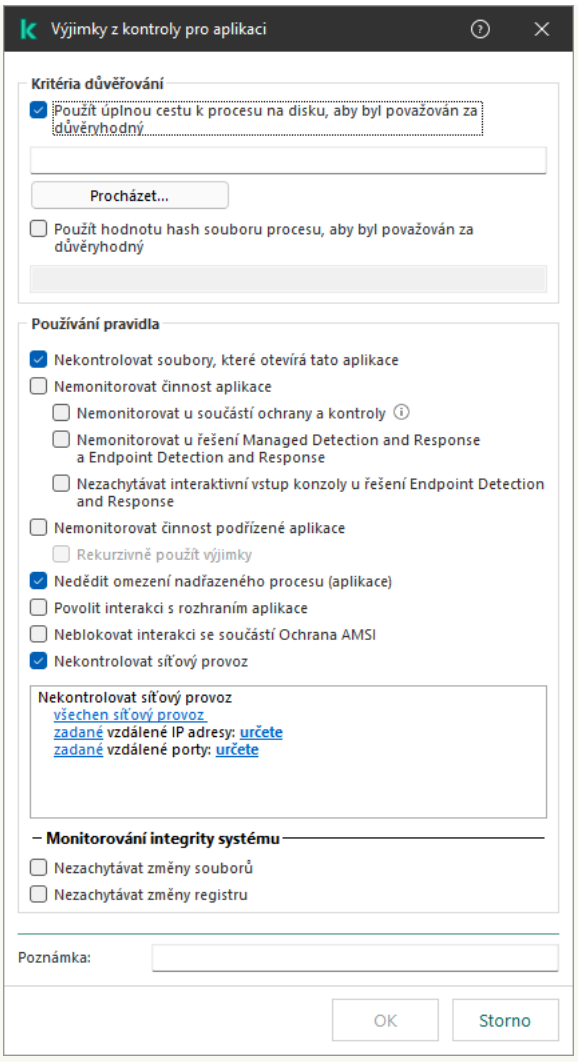
   - **Použít úplnou cestu k procesu na disku, aby byl považován za důvěryhodný**. Zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

     Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

     Aplikace Kaspersky Endpoint Security u názvu souboru důvěryhodné aplikace rozlišuje velká a malá písmena. Pokud má zadaný název souboru nesprávně velká a malá písmena, aplikace Kaspersky Endpoint Security nerozpozná důvěryhodnou aplikaci.

   - **Použít hodnotu hash souboru procesu, aby byl považován za důvěryhodný**.

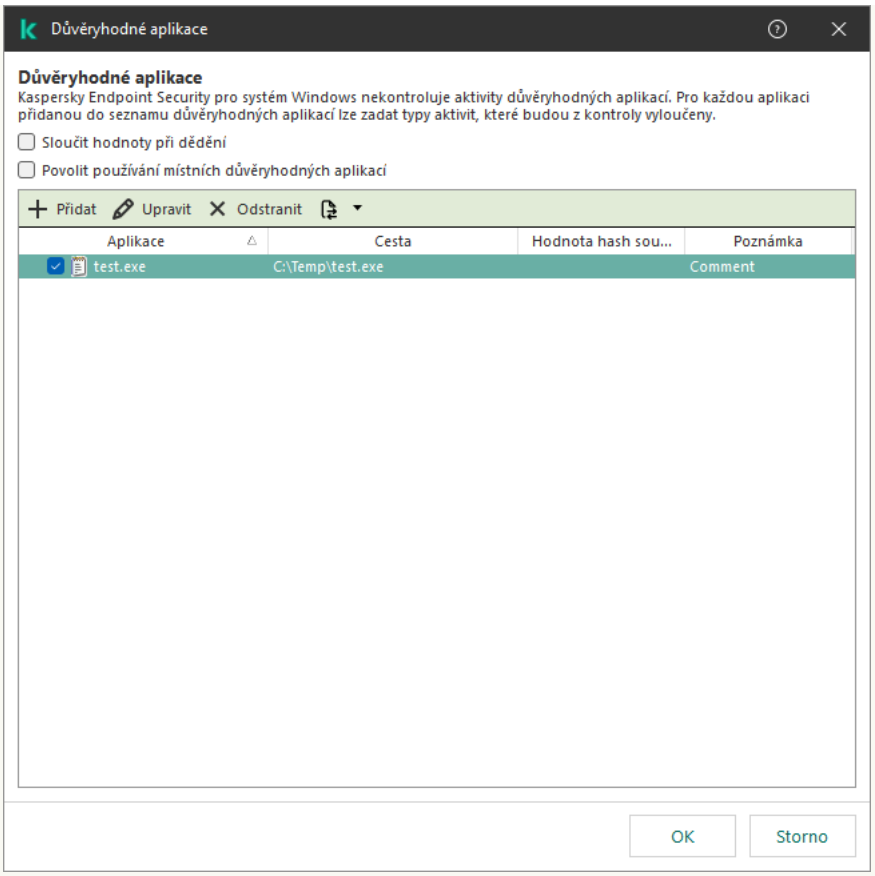
   Kaspersky Endpoint Security nepodporuje při generování seznamu důvěryhodných aplikací v konzole aplikace Kaspersky Security Center proměnnou prostředí `%userprofile%`. Chcete-li položku použít na všechny uživatelské účty, můžete použít znak * (například `C:\Users\*\Documents\File.exe`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.



Nastavení důvěryhodné aplikace

9. Nakonfigurujte rozšířené nastavení pro důvěryhodnou aplikaci (viz tabulka níže).
10. Klikněte na tlačítko **OK**.

    Nová důvěryhodná aplikace bude přidána do seznamu. Aplikaci můžete z důvěryhodné zóny kdykoli vyloučit pomocí zaškrtávacího políčka vedle objektu.
11. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.



Seznam důvěryhodných aplikací

[Jak přidat aplikaci na seznam důvěryhodných aplikací ve webové konzole a cloudové konzole](#)

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **Trusted Zone**.
5. V okně, které se otevře, klikněte na odkaz **Applications**.

   Otevře se okno obsahující seznam důvěryhodných aplikací.
6. Pokud chcete vytvořit konsolidovaný seznam důvěryhodných aplikací pro všechny počítače ve společnosti, zaškrtněte políčko **Merge values when inheriting**. 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 **Allow use of local exclusions**. 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 toto políčko není zaškrtnuté, Kaspersky Endpoint Security skryje konsolidovaný seznam důvěryhodných aplikací v uživatelském rozhraní aplikace.
8. Klikněte na tlačítko **Add** a vyberte akci:

   - **Category**. Důvěryhodné aplikace můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu důvěryhodnou aplikaci.
   - **New exclusion**. Aplikace Kaspersky Endpoint Security přidá novou důvěryhodnou aplikaci do kořenového seznamu.
   - **Select exclusion from list**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované důvěryhodné aplikace*. Byly také přidány důvěryhodné aplikace z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované důvěryhodné aplikace.

Chcete-li přidat novou důvěryhodnou aplikaci do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **New exclusion**.

9. Vyberte kritéria důvěry:

   - **Path to the file or folder**. Zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

     Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

     Aplikace Kaspersky Endpoint Security u názvu souboru důvěryhodné aplikace rozlišuje velká a malá písmena. Pokud má zadaný název souboru nesprávně velká a malá písmena, aplikace Kaspersky Endpoint Security nerozpozná důvěryhodnou aplikaci.

   - **Application hash**.

   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`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

10. Nakonfigurujte rozšířené nastavení pro důvěryhodnou aplikaci (viz tabulka níže).

11. Klikněte na tlačítko **OK**.

    Nová důvěryhodná aplikace bude přidána do seznamu. Aplikaci můžete z důvěryhodné zóny kdykoli vyloučit pomocí zaškrtávacího políčka ve sloupci **Status**.

12. Uložte změny.

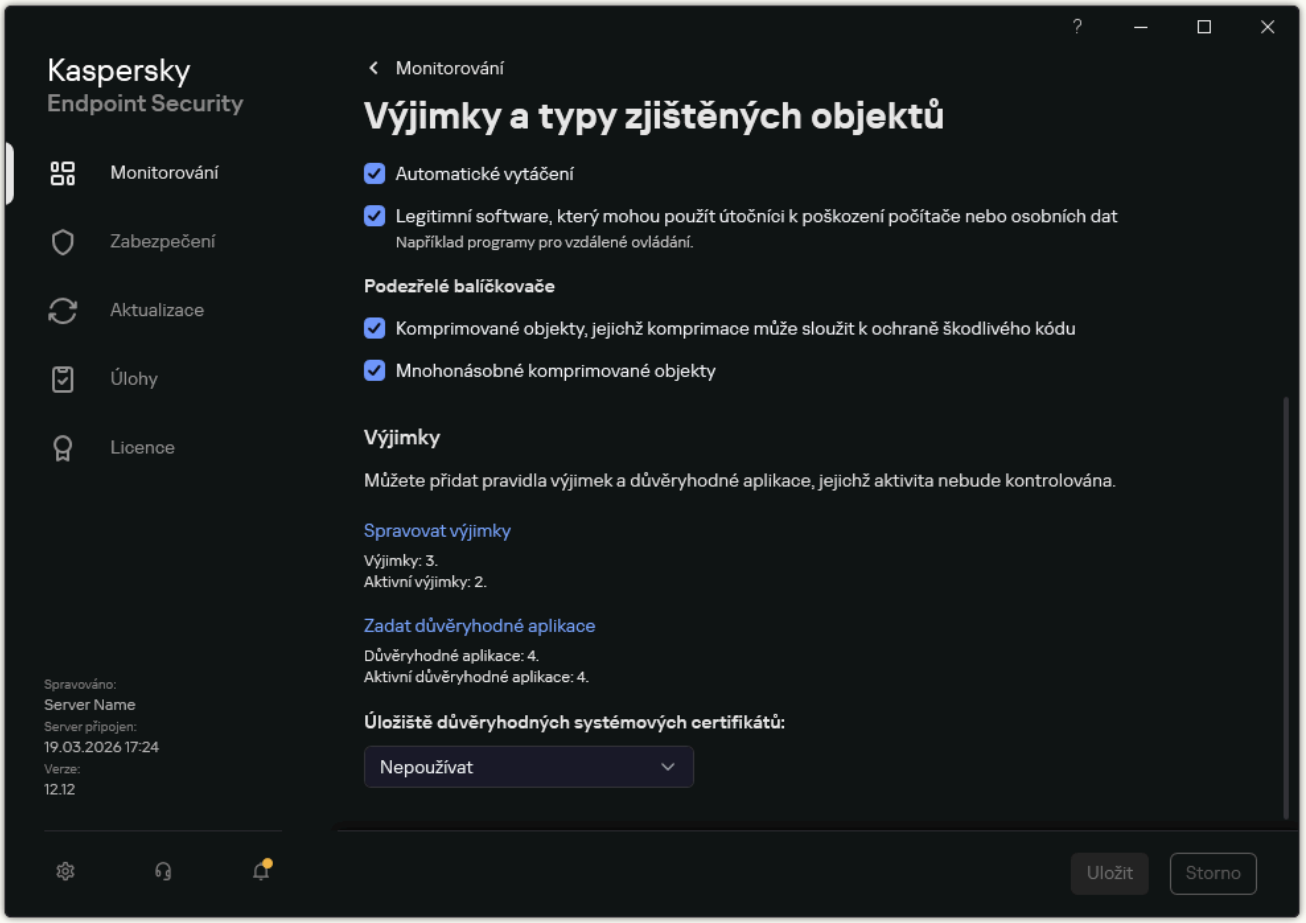
Jak přidat aplikaci na seznam důvěryhodných v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.

3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.

   Kaspersky Endpoint Security skryje konsolidovaný seznam důvěryhodných aplikací v uživatelském rozhraní aplikace, pokud je konfigurace důvěryhodných aplikací blokována správcem v konzole (symbol „zavřeného zámku") a místní důvěryhodné aplikace jsou zakázány (není zaškrtnuto políčko **Povolit používání místních důvěryhodných aplikací**).



Nastavení výjimek

4. Klikněte na tlačítko **Přidat** a vyberte akci:

- **Kategorie**. Důvěryhodné aplikace můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu důvěryhodnou aplikaci.
- **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou důvěryhodnou aplikaci do kořenového seznamu.
- **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované důvěryhodné aplikace*. Byly také přidány důvěryhodné aplikace z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované důvěryhodné aplikace.

Chcete-li přidat novou důvěryhodnou aplikaci do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **Nová výjimka**.

5. Vyberte kritéria důvěry:

- **Použít úplnou cestu k procesu na disku, aby byl považován za důvěryhodný**. Zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

  Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

  Aplikace Kaspersky Endpoint Security u názvu souboru důvěryhodné aplikace rozlišuje velká a malá písmena. Pokud má zadaný název souboru nesprávně velká a malá písmena, aplikace Kaspersky Endpoint Security nerozpozná důvěryhodnou aplikaci.

- **Použít hodnotu hash souboru procesu, aby byl považován za důvěryhodný**.

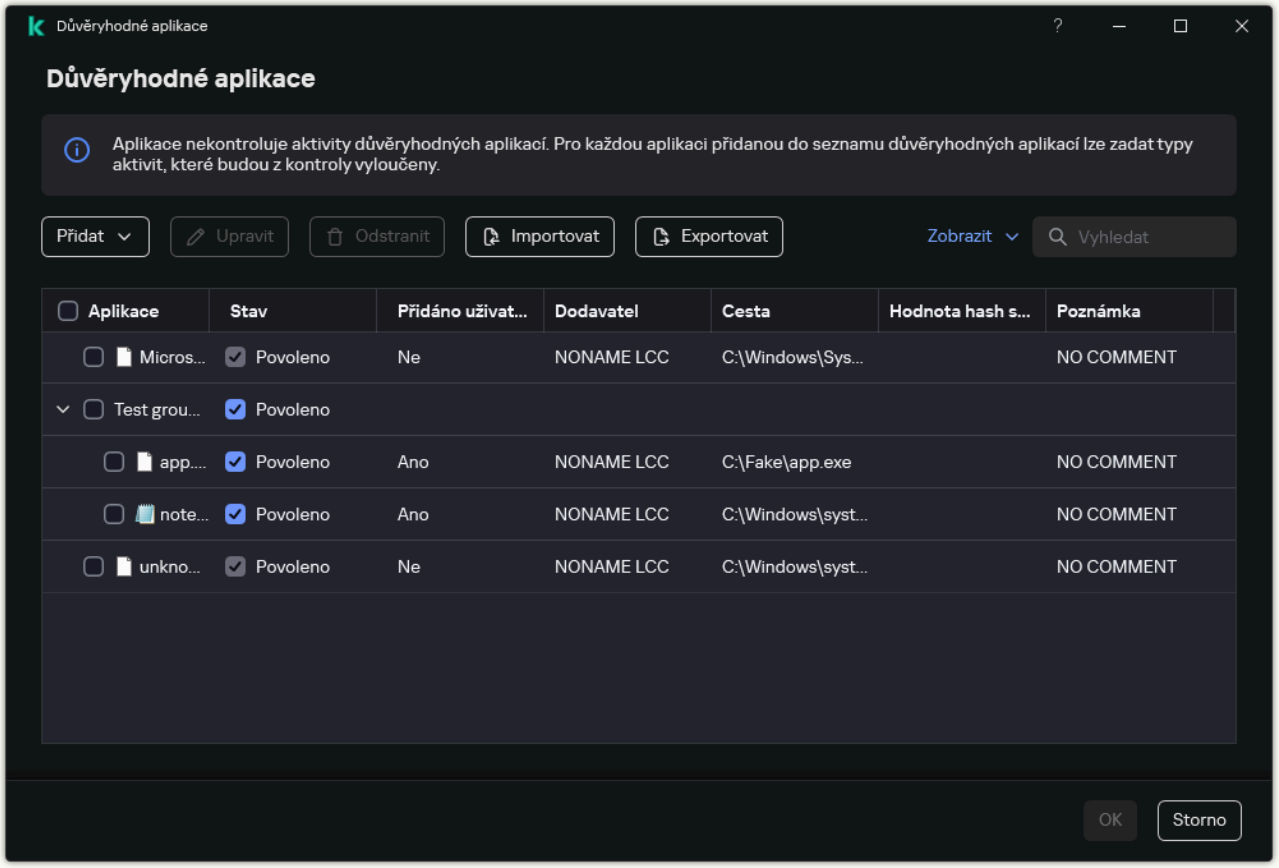
Aplikace Kaspersky Endpoint Security podporuje proměnné prostředí a převádí cestu v místním rozhraní aplikace. Jinými slovy, pokud zadáte cestu k souboru `%userprofile%\Documents\File.exe`, do místního rozhraní aplikace pro uživatele Fred123 se přidá záznam `C:\Users\Fred123\Documents\File.exe`. Kaspersky Endpoint Security tak bude ignorovat důvěryhodný program `File.exe` u jiných uživatelů. chcete-li položku použít na všechny uživatelské účty, můžete použít znak `*` (například `C:\Users\*\Documents\File.exe`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

6. V okně vlastností důvěryhodné aplikace nakonfigurujte rozšířené nastavení.

7. Klikněte na tlačítko **OK**.

Nová důvěryhodná aplikace bude přidána do seznamu. Aplikaci můžete z důvěryhodné zóny kdykoli vyloučit pomocí zaškrtávacího políčka ve sloupci **Stav**.

8. Uložte změny.



Seznam důvěryhodných aplikací

Nastavení důvěryhodné aplikace

Parametr	Popis
Nekontrolovat soubory, které otevírá tato aplikace	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.
Nemonitorovat činnost aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat souborovou ani síťovou aktivitu aplikace v operačním systému. Monitorování aktivity aplikací můžete nakonfigurovat pro různé součásti aplikace Kaspersky Endpoint Security: • **Nemonitorovat u součástí ochrany a kontroly**. Činnost aplikace je monitorována následujícími součástmi: Detekce chování, Prevence zneužití, Prevence narušení hostitele, Modul pro nápravu a Brána firewall. • **Nemonitorovat u řešení Managed Detection and Response a Endpoint Detection and Response**. Aktivitu aplikace monitoruje integrovaný agent MDR a integrovaný agent EDR (KATA). • **Nezachytávat interaktivní vstup konzoly u řešení Endpoint Detection and Response**. Kaspersky Endpoint Security neodesílá telemetrická data o správě aplikace na konzole. Telemetrická data používá platformou Kaspersky Anti Targeted Attack Platform (EDR).
Nemonitorovat činnost podřízené aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu souborů ani síťovou aktivitu aplikací spuštěných touto aplikací. Výjimku můžete použít rekurzivně. Aplikace tak nebude monitorovat činnost celého řetězce podřízených aplikací.
Nedědit omezení z 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).
Nemonitorovat činnost podřízené aplikace	Aplikace Kaspersky Endpoint Security nebude monitorovat aktivitu souborů ani síťovou aktivitu aplikací spuštěných touto aplikací. Výjimku můžete použít rekurzivně. Aplikace tak nebude monitorovat činnost celého řetězce podřízených aplikací.
Povolit interakci s rozhraním aplikace	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.
Neblokovat interakci se součástí Ochrana AMSI	Aplikace Kaspersky Endpoint Security nebude monitorovat požadavky důvěryhodné aplikace na objekty, které mají být kontrolovány součástí Ochrana AMSI.

Nekontrolovat síťový 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. Pokud je pro důvěryhodnou aplikaci místo cesty zadána hodnota hash, aplikace nepodporuje vyloučení síťového provozu.
Nezachytávat změny souborů *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Aplikace Kaspersky Endpoint Security nesleduje změny v souborech z rozsahu monitorování Monitorování integrity systému. Aplikace použije výjimku na všechny režimy Monitorování integrity systému: Monitorování integrity systému v reálném čase a Kontrola integrity systému na vyžádání.
Nezachytávat změny registru *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Aplikace Kaspersky Endpoint Security nesleduje změny v klíčích registru z rozsahu monitorování Monitorování integrity systému. Aplikace použije výjimku na všechny režimy Monitorování integrity systému: Monitorování integrity systému v reálném čase a Kontrola integrity systému na vyžádání.
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.

Vytvoření místní důvěryhodné zóny

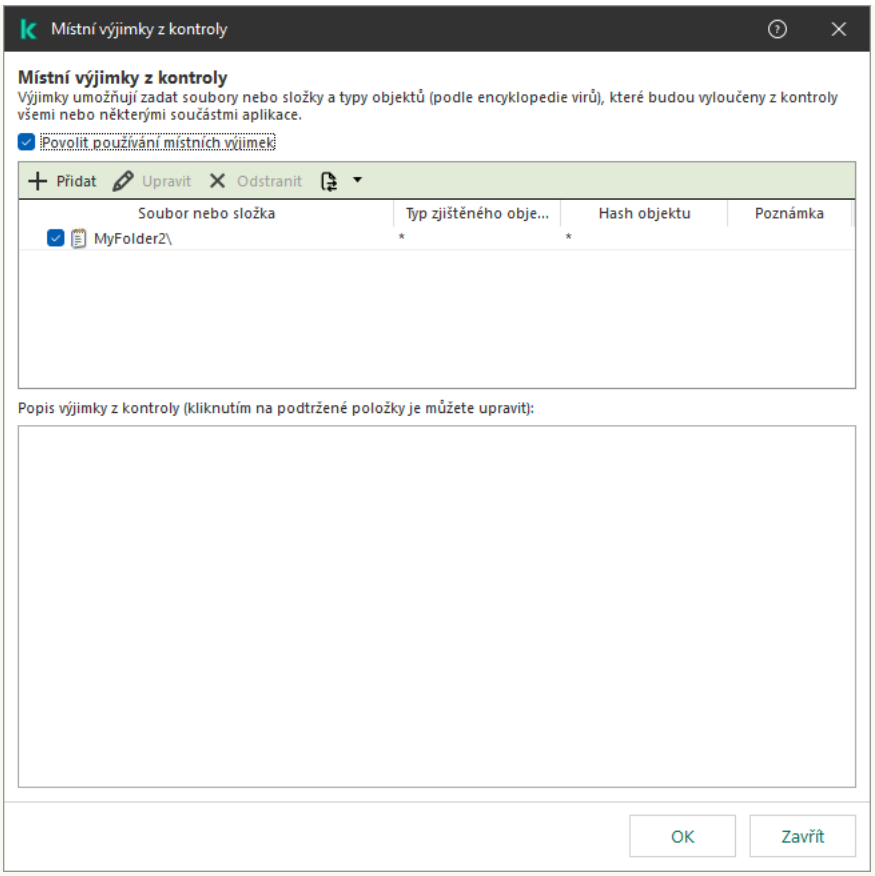
Uživatel nově může vytvořit svou vlastní místní důvěryhodnou zónu pro konkrétní počítač. Uživatelé tak mohou kromě obecné důvěryhodné zóny v zásadách vytvářet také vlastní místní seznamy výjimek a důvěryhodných aplikací. Správce může v nastavení zásad povolit nebo zablokovat použití místních výjimek nebo místních důvěryhodných aplikací. K tomu slouží zaškrtávací políčka **Povolit používání místních výjimek** a **Povolit používání místních důvěryhodných aplikací** v části **Výjimky** zásad.

Pokud vytvoření místní důvěryhodné zóny povolí správce, uživatel může v uživatelském rozhraní aplikace přidat vlastní výjimky z kontroly a důvěryhodné aplikace. Uživatel zároveň nemá oprávnění upravovat ani odstraňovat objekty z důvěryhodné zóny nakonfigurované v zásadách. Správce může také zobrazit, přidat, upravit nebo odstranit položky seznamu v konzole aplikace Kaspersky Security Center, pokud je třeba přidat výjimky pro jednotlivý počítač.

Kaspersky Endpoint Security skryje seznamy výjimek z kontroly a důvěryhodných aplikací v uživatelském rozhraní aplikace, pokud je konfigurace důvěryhodné zóny blokována správcem v konzole (symbol „zavřeného zámku") a místní výjimky z kontroly a důvěryhodné aplikace jsou zakázány.

Jak přidat objekt do místní důvěryhodné zóny 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. 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 (14.0)** a dvojitým kliknutím otevřete vlastnosti aplikace.
7. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Výjimky a typy objektů**.
8. V bloku **Výjimky z kontroly a důvěryhodné aplikace → Místní výjimky z kontroly** klikněte na tlačítko **Nastavení**.
   Otevře se okno obsahující seznam místních výjimek.



Nastavení důvěryhodné zóny

9. Vytvořte seznam místních výjimek z kontroly.

   Pravidla pro vytváření místních výjimek z kontroly jsou stejná jako u obecných výjimek. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

10. V bloku **Výjimky z kontroly a důvěryhodné aplikace** → **Místní důvěryhodné aplikace** klikněte na tlačítko **Nastavení**.

    Otevře se okno obsahující seznam místních důvěryhodných aplikací.

11. Vytvořte seznam místních důvěryhodných aplikací.

    Pravidla pro přidávání aplikací na seznam místních důvěryhodných aplikací jsou stejná jako pravidla pro jejich přidávání na obecný seznam. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

12. Uložte změny.

Jak přidat objekt do místní důvěryhodné zóny ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Klikněte na název počítače, u něhož chcete uživateli povolit provedení blokované akce.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.

   Otevřou se místní nastavení aplikace.

5. Vyberte kartu **Application settings**.
6. V okně nastavení aplikace vyberte možnost **General settings** → **Exclusions and types of detected objects**.
7. V bloku **Scan exclusions and trusted applications** klikněte na odkaz **Local scan exclusions**.
8. Vytvořte seznam místních výjimek z kontroly.

   Pravidla pro vytváření místních výjimek jsou stejná jako u pravidla pro vytváření obecných výjimek. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

9. V bloku **Scan exclusions and trusted applications** klikněte na odkaz **Local trusted applications**.

10. Vytvořte seznam místních důvěryhodných aplikací.

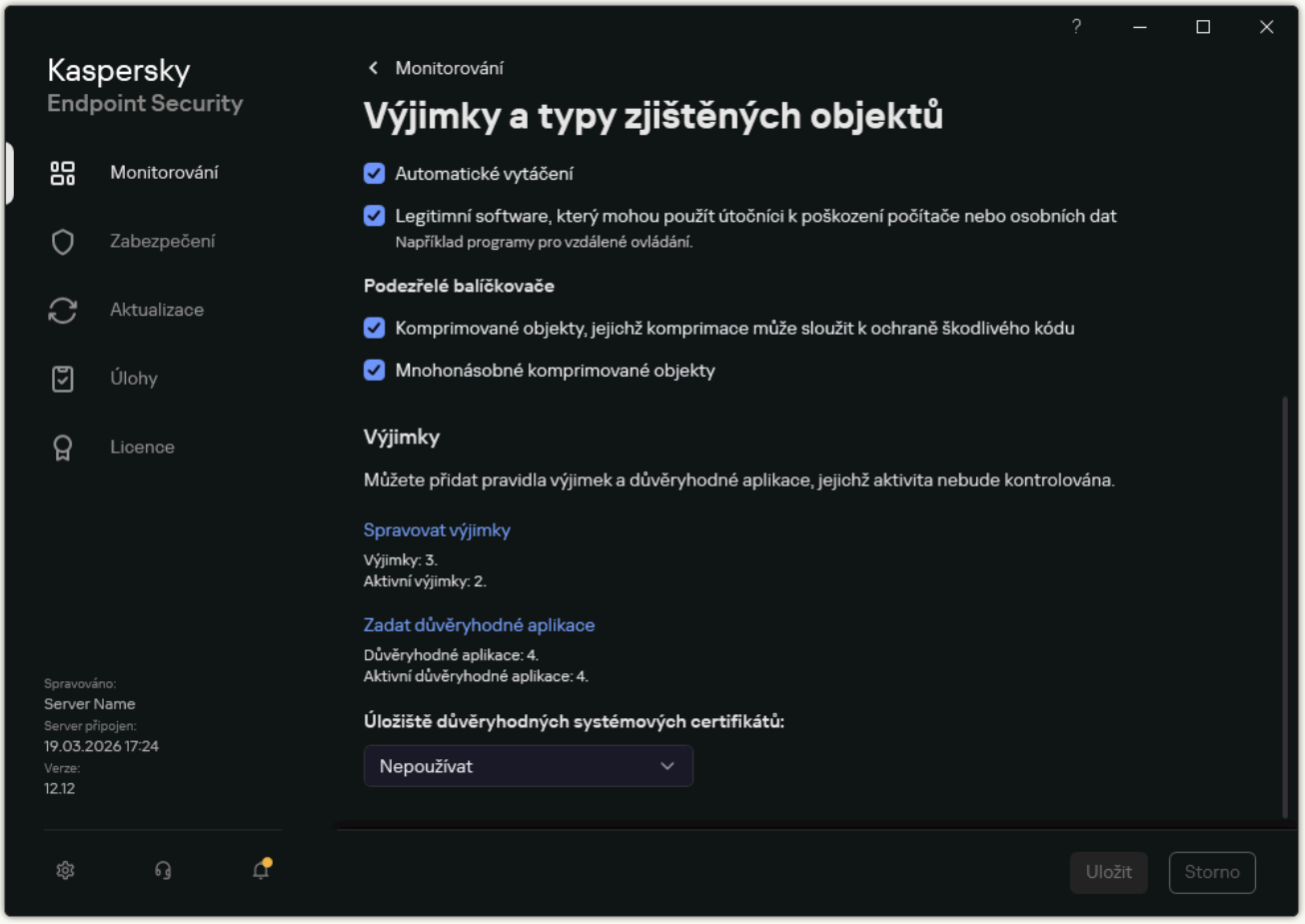
    Pravidla pro přidávání aplikací na seznam místních důvěryhodných aplikací jsou stejná jako pravidla pro jejich přidávání na obecný seznam. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

11. Uložte změny.

Jak vytvořit místní výjimku z kontroly v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.
3. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.

   Kaspersky Endpoint Security skryje seznam výjimek z kontroly v uživatelském rozhraní aplikace, pokud je konfigurace výjimek z kontroly blokována správcem v konzole (symbol „zavřeného zámku“) a místní výjimky z kontroly jsou zakázány (není zaškrtnuto políčko **Povolit používání místních výjimek**).



Nastavení výjimek

4. Klikněte na tlačítko **Přidat** a vyberte akci:

   - **Kategorie**. Výjimky z kontroly můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu výjimku z kontroly.
   - **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou výjimku z kontroly do kořenového seznamu.
   - **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované výjimky z kontroly*. Byly také přidány předdefinované výjimky z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované výjimky z kontroly.

   Chcete-li přidat novou výjimku z kontroly do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **Nová výjimka**.

5. Pokud chcete z kontroly vyloučit soubor nebo složku, vyberte je po kliknutí na tlačítko **Procházet**.

Cestu můžete rovněž zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

  Masky můžete použít na začátku, uprostřed nebo na konci cesty k souboru. Chcete-li například do výjimky přidat složku pro všechny uživatele, zadejte masku `?:\Users\*\Folder\`.

  Síťové složky můžete vyloučit. To provedete tak, že ručně zadáte cestu k síťové složce (např. `\\Network Share\*`).

6. Chcete-li z kontroly vyloučit určitý typ objektu, zadejte do pole **Typ zjištěného objektu** 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 **Hash objektu** 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.

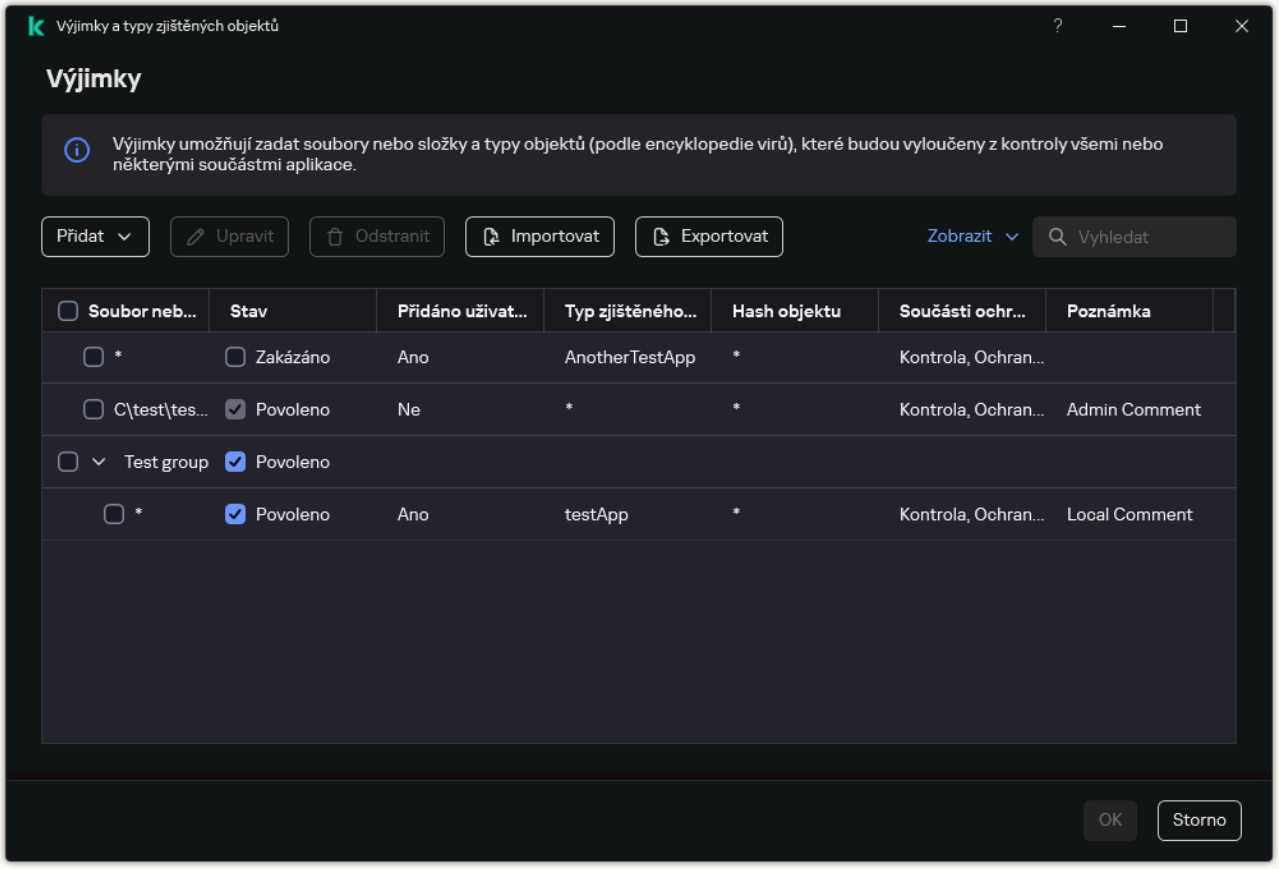
9. V případě potřeby zadejte k vytvářené výjimce z kontroly stručný komentář do pole **Poznámka**.

10. Vyberte pro výjimku stav **Aktivní**.

11. Klikněte na tlačítko **Přidat**.

    Nová výjimka bude přidána do seznamu. Výjimku můžete kdykoli zakázat pomocí zaškrtávacího políčka vedle sloupce **Stav**.

12. Uložte změny.

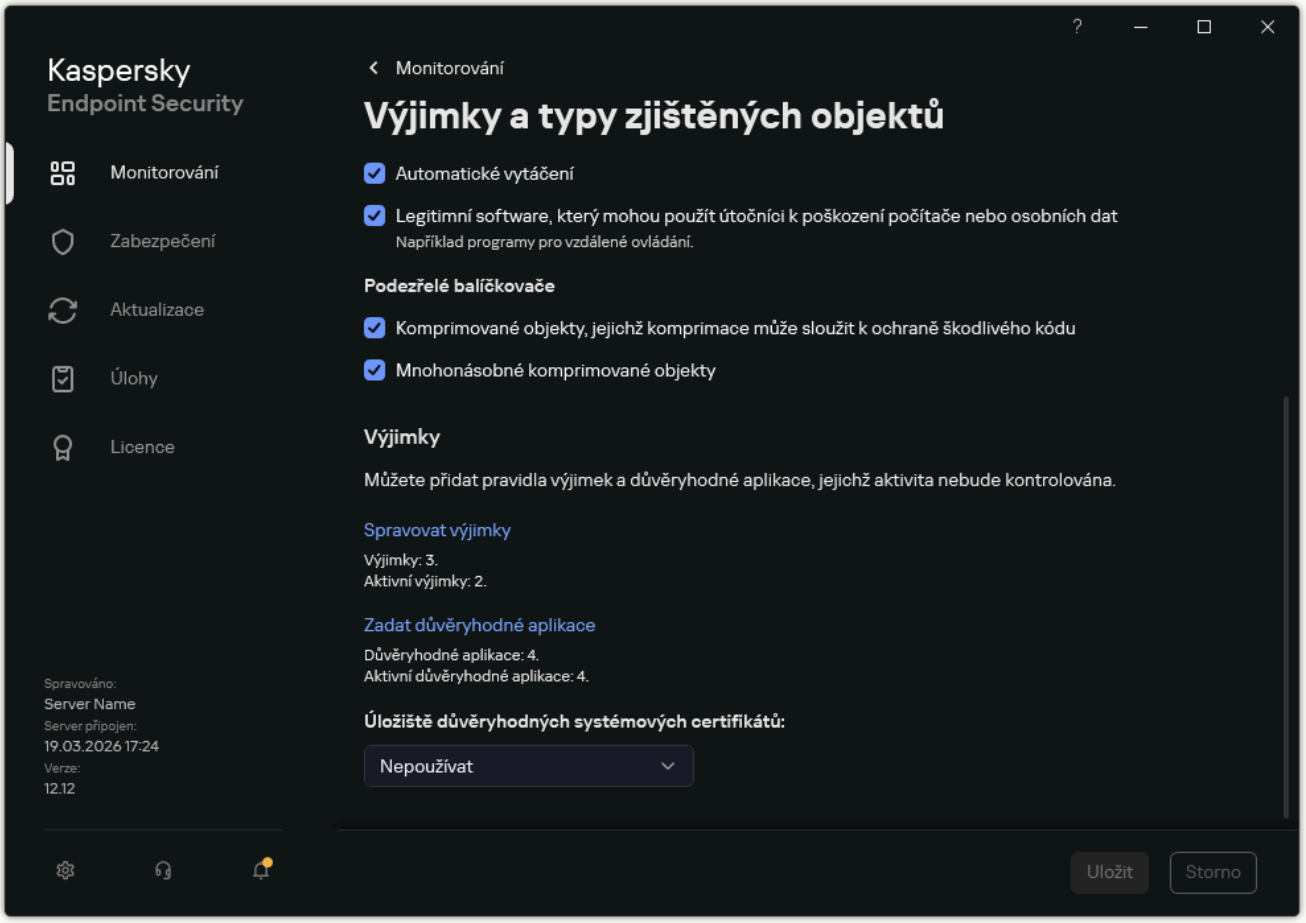


Seznam výjimek

Jak přidat aplikaci na seznam místních důvěryhodných aplikací v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Výjimky a typy zjištěných objektů**.
3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.

   Kaspersky Endpoint Security skryje konsolidovaný seznam důvěryhodných aplikací v uživatelském rozhraní aplikace, pokud je konfigurace důvěryhodných aplikací blokována správcem v konzole (symbol „zavřeného zámku") a místní důvěryhodné aplikace jsou zakázány (není zaškrtnuto políčko **Povolit používání místních důvěryhodných aplikací**).



Nastavení výjimek

4. Klikněte na tlačítko **Přidat** a vyberte akci:

   - **Kategorie**. Důvěryhodné aplikace můžete seskupit do samostatných kategorií. Chcete-li vytvořit novou kategorii, zadejte název kategorie a přidejte do kategorie alespoň jednu důvěryhodnou aplikaci.
   - **Nová výjimka**. Aplikace Kaspersky Endpoint Security přidá novou důvěryhodnou aplikaci do kořenového seznamu.
   - **Vyberte výjimku ze seznamu**. Chcete-li rychle nakonfigurovat Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a v řešení System Center Configuration Manager, aplikace obsahuje *předdefinované důvěryhodné aplikace*. Byly také přidány důvěryhodné aplikace z kontroly pro podporu nastavení aplikací ve virtuálních prostředích Citrix a VMware. V závislosti na účelu chráněného serveru musíte vybrat předdefinované důvěryhodné aplikace.

   Chcete-li přidat novou důvěryhodnou aplikaci do konkrétní kategorie, zaškrtněte políčko vedle této kategorie a vyberte možnost **Nová výjimka**.

5. Vyberte kritéria důvěry:

   - **Použít úplnou cestu k procesu na disku, aby byl považován za důvěryhodný**. Zadejte cestu ke spustitelnému souboru důvěryhodné aplikace.

     Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.

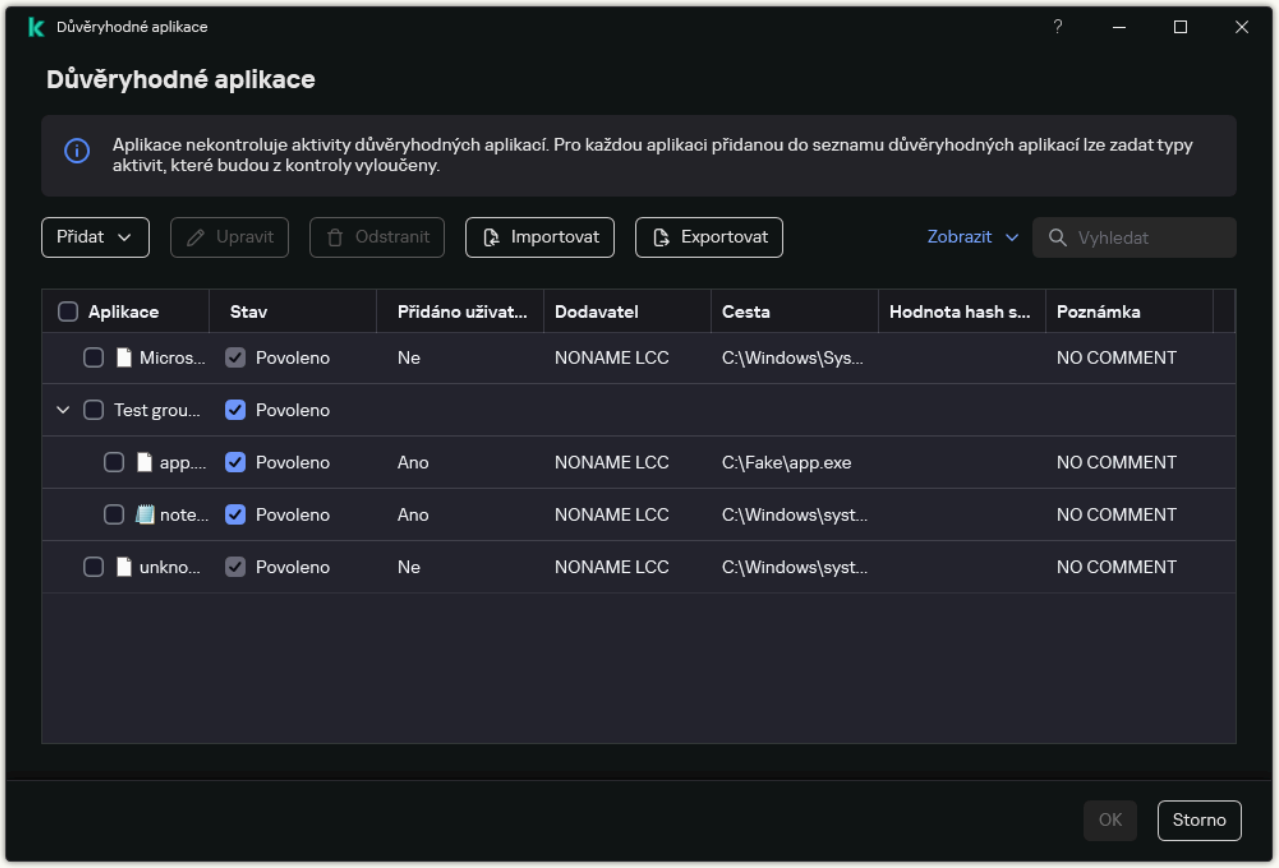
     Aplikace Kaspersky Endpoint Security u názvu souboru důvěryhodné aplikace rozlišuje velká a malá písmena. Pokud má zadaný název souboru nesprávně velká a malá písmena, aplikace Kaspersky Endpoint Security nerozpozná důvěryhodnou aplikaci.

- **Použít hodnotu hash souboru procesu, aby byl považován za důvěryhodný**.

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 všechny uživatelské účty, můžete použít znak `*` (například `C:\Users\*\Documents\File.exe`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

6. V okně vlastností důvěryhodné aplikace nakonfigurujte rozšířené nastavení.
7. Klikněte na tlačítko **OK**.

   Nová důvěryhodná aplikace bude přidána do seznamu. Aplikaci můžete z důvěryhodné zóny kdykoli vyloučit pomocí zaškrtávacího políčka ve sloupci **Stav**.
8. Uložte změny.



Seznam důvěryhodných aplikací

Export a import důvěryhodné zóny

Důvěryhodná zóna je správcem konfigurovaný seznam objektů a aplikací, které aplikace Kaspersky Endpoint Security nesleduje, když jsou aktivní. Důvěryhodná zóna se skládá z následujících seznamů: *výjimky z kontroly* a *důvěryhodné aplikace*. Tyto seznamy můžete exportovat do souborů XML a dalších formátů. Pak můžete soubor upravit, například přidat velké množství výjimek stejného typu. Funkci exportu/importu můžete také použít k zálohování seznamu výjimek a seznamu důvěryhodných aplikací nebo k migraci seznamů na jiný server.

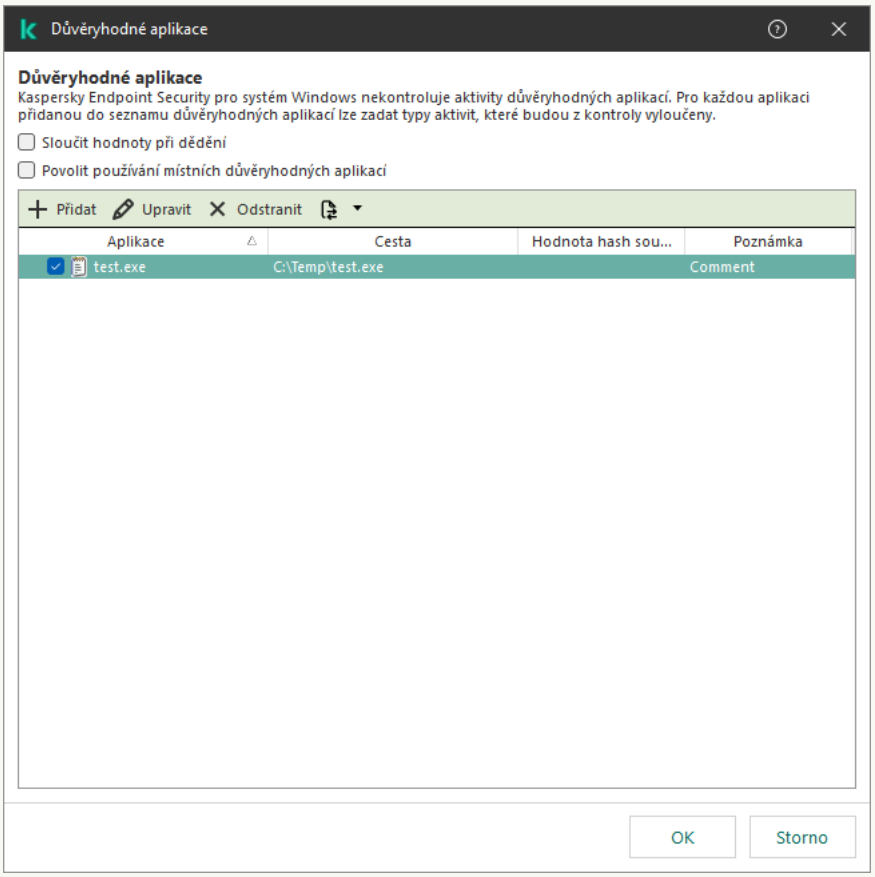
Aplikace používá pro export a import *seznamu výjimek* tyto formáty:

- XML je k dispozici v konzole pro správu (MMC), webové konzole a cloudové konzole.
- DAT je k dispozici pouze pro import v konzole pro správu (MMC). Účelem tohoto formátu je zachovat kompatibilitu se staršími verzemi aplikace. Chcete-li migrovat seznamy výjimek do webové konzoly, můžete v konzole pro správu (MMC) převést soubor DAT na XML.
- CSV je k dispozici pouze v místním rozhraní aplikace.

Aplikace Kaspersky Endpoint Security používá pro export a import *seznamu důvěryhodných aplikací* formát XML.

Jak exportovat a importovat důvěryhodnou zónu v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
4. V části **Výjimky z kontroly a důvěryhodné aplikace** vyberte součást důvěryhodné zóny, kterou chcete exportovat nebo importovat: **Výjimky z kontroly** nebo **Důvěryhodné aplikace**.
5. Klikněte na tlačítko **Nastavení**.
6. 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 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. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML. Aplikace Kaspersky Endpoint Security rovněž podporuje export seznamu výjimek do souboru DAT.



Seznam důvěryhodných aplikací

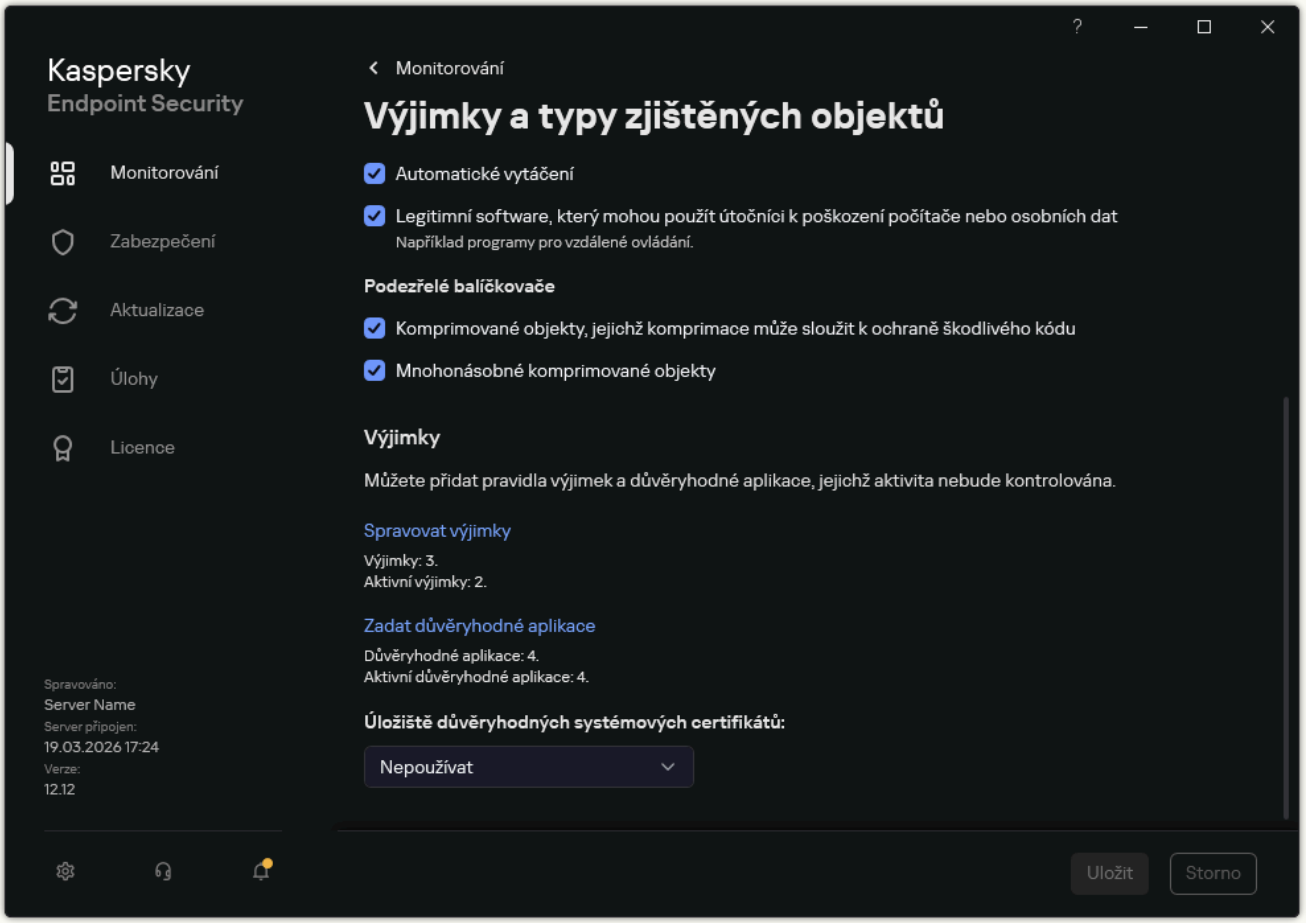
7. Postup importu seznamu výjimek:
   a. Klikněte na tlačítko → **Importovat**.
   b. V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam výjimek.
   c. Otevřete soubor.
      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky. Aplikace Kaspersky Endpoint Security rovněž podporuje import seznamu výjimek ze souboru DAT.
8. Uložte změny.

Jak exportovat nebo importovat důvěryhodnou zónu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **Trusted Zone**.
5. Postup exportu seznamu pravidel:
   a. Klikněte na odkaz **Malware Scan exclusions**.
   b. Vyberte výjimky, které chcete exportovat.
   c. Klikněte na tlačítko → **Export**.
      Aplikace Kaspersky Endpoint Security exportuje seznam výjimek do souboru JSON ve výchozí složce pro stahování.
6. Postup exportu seznamu důvěryhodných aplikací:
   a. Vyberte důvěryhodné aplikace, které chcete exportovat.
   b. Klikněte na tlačítko → **Export**.
      Aplikace Kaspersky Endpoint Security exportuje seznam důvěryhodných aplikací do souboru JSON ve výchozí složce pro stahování.
7. Postup importu seznamu výjimek:
   a. Klikněte na odkaz **Malware Scan exclusions**.
   b. Klikněte na tlačítko → **Import**.
      V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam výjimek.
   c. Otevřete soubor.
      Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru JSON přidá nové položky.
8. Postup importu seznamu důvěryhodných aplikací:
   a. Klikněte na odkaz **Applications**.
   b. Klikněte na tlačítko → **Import**.
      Tato akce otevře okno; v tomto okně vyberte soubor JSON, ze kterého chcete importovat seznam důvěryhodných aplikací.
   c. Otevřete soubor.
      Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru JSON přidali nové položky.
9. Uložte změny.

Jak exportovat nebo importovat důvěryhodnou zónu v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.



Nastavení výjimek

3. Postup exportu seznamu pravidel:

   a. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.

   b. Vyberte výjimky, které chcete exportovat.

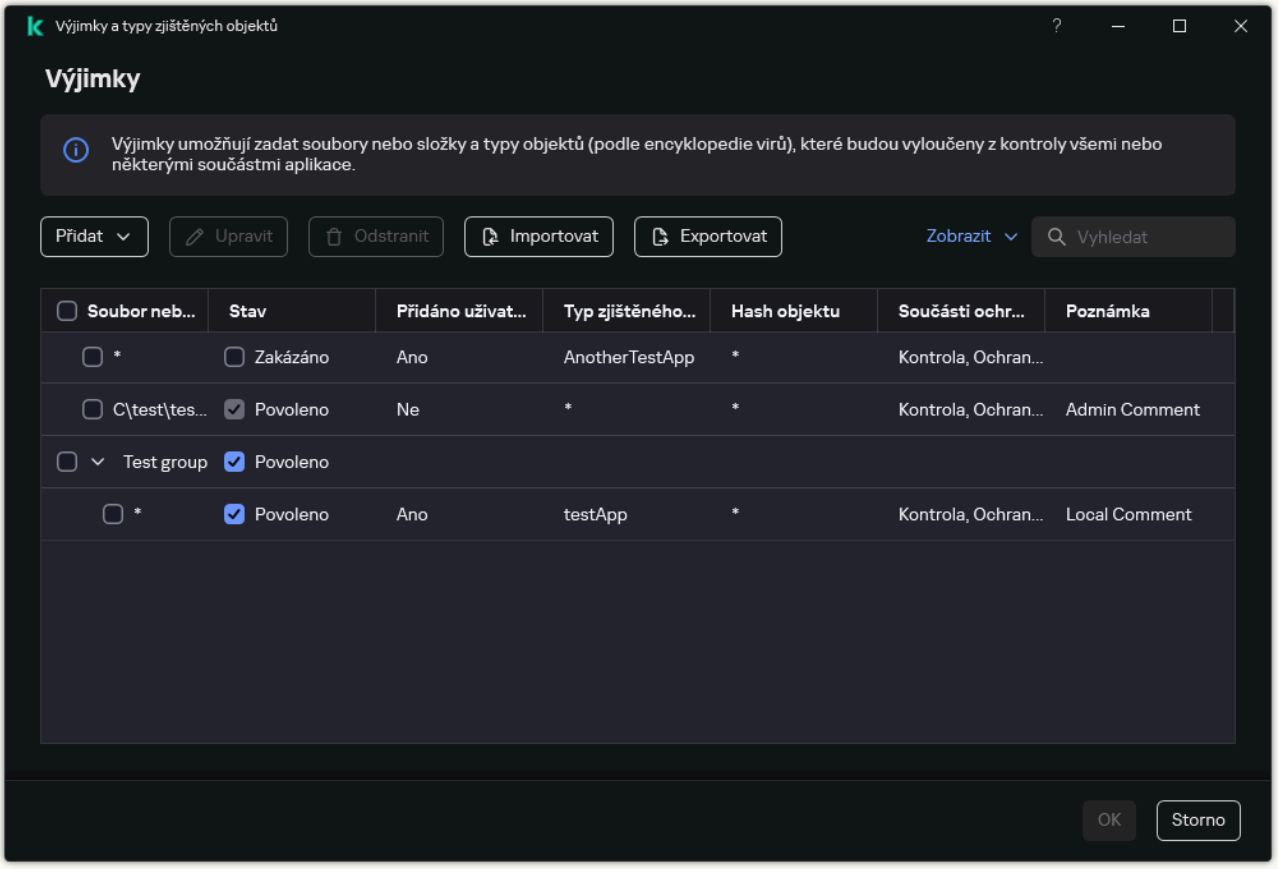
   c. Klikněte na tlačítko **Exportovat**.

   d. Potvrd'te, jestli chcete exportovat pouze vybrané výjimky, nebo exportovat celý seznam výjimek.

   e. V okně, které se otevře, zadejte název souboru CSV, do kterého chcete exportovat seznam výjimek, a vyberte složku, do které chcete tento soubor uložit.

   f. Uložte soubor.

      Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru CSV.



Seznam výjimek

4. Postup exportu seznamu důvěryhodných aplikací:

   a. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.

   b. Vyberte důvěryhodné aplikace, které chcete exportovat.

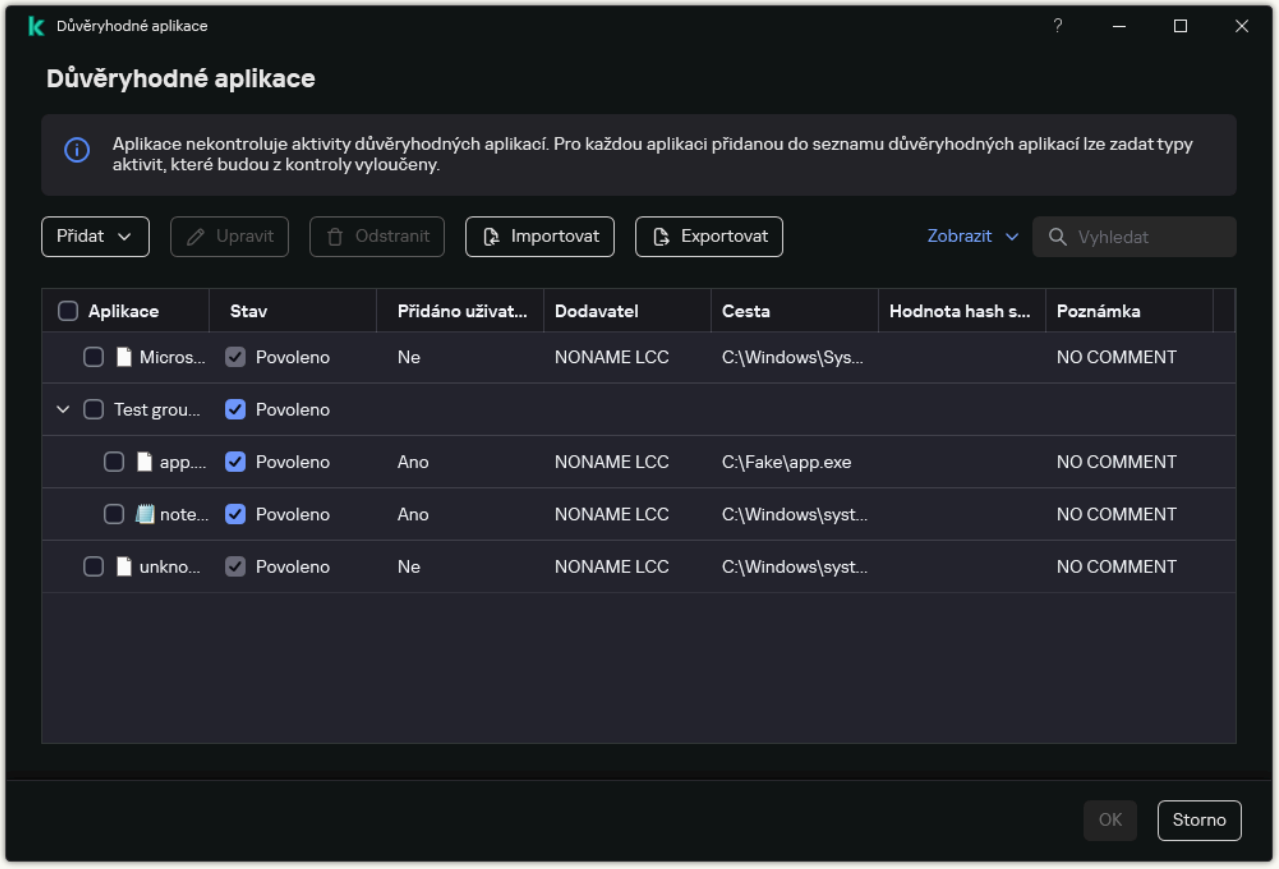
   c. Klikněte na tlačítko **Exportovat**.

   d. Potvrďte, jestli chcete exportovat pouze vybrané důvěryhodné aplikace, nebo exportovat celý seznam.

   e. Tato akce otevře okno; v tomto okně zadejte název souboru XML, do kterého chcete exportovat seznam důvěryhodných aplikací, a vyberte složku, do které chcete tento soubor uložit.

   f. Uložte soubor.

   Aplikace Kaspersky Endpoint Security exportuje celý seznam důvěryhodných aplikací do souboru XML.



Seznam důvěryhodných aplikací

5. Postup importu seznamu výjimek:

   a. V bloku **Výjimky** klikněte na odkaz **Spravovat výjimky**.

   b. Klikněte na tlačítko **Importovat**.

   c. V okně, které se otevře, vyberte soubor CSV, ze kterého chcete importovat seznam výjimek.

   d. Otevřete soubor.

   Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru CSV přidá nové položky.

6. Postup importu seznamu důvěryhodných aplikací:

   a. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.

   b. Klikněte na tlačítko **Importovat**.

   c. Tato akce otevře okno; v tomto okně vyberte soubor XML, ze kterého chcete importovat seznam důvěryhodných aplikací.

   d. Otevřete soubor.

   Pokud počítač již seznam důvěryhodných aplikací obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

7. Uložte změny.

Zpracování aplikací s důvěryhodným digitálním podpisem

Použití úložiště certifikátů systému umožňuje vyjmout aplikace s důvěryhodným digitálním podpisem z antivirových kontrol. Kaspersky Endpoint Security automaticky přiřadí takové aplikace do skupiny *Důvěryhodné*.

Jak začít používat úložiště důvěryhodných systémových certifikátů v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
4. V bloku **Úložiště důvěryhodných systémových certifikátů** zaškrtněte políčko **Použít úložiště důvěryhodných systémových certifikátů**.
5. V rozevíracím seznamu vyberte, které systémové úložiště má aplikace Kaspersky Endpoint Security považovat za důvěryhodné.
6. Uložte změny.

Jak začít používat úložiště důvěryhodných systémových certifikátů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **Trusted Zone**.
5. V okně, které se otevře, klikněte na odkaz **Trusted certificates**.
6. V okně, které se otevře, zaškrtněte políčko **Use trusted system certificate store**.
7. Vyberte, které systémové úložiště má aplikace Kaspersky Endpoint Security považovat za důvěryhodné.
8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak začít používat úložiště důvěryhodných systémových certifikátů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.
3. V rozevíracím seznamu **Úložiště důvěryhodných systémových certifikátů** vyberte, které systémové úložiště má aplikace Kaspersky Endpoint Security považovat za důvěryhodné.
4. Uložte změny.

Příloha Předdefinované výjimky z kontroly a důvěryhodné aplikace

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware.

Předdefinované výjimky a důvěryhodné aplikace můžete vybrat následujícími způsoby:

- Instalace aplikace.
  - Místní instalace aplikace pomocí průvodce
  - Vlastností instalačního balíčku
- Nastavení zásad.
  - Průvodce novou zásadou
  - Vlastnosti zásad: výjimky z kontroly a důvěryhodné aplikace

Server SQL

Při instalaci aplikace Kaspersky Endpoint Security na server SQL musíte vytvořit důvěryhodnou zónu z předdefinovaných výjimek a důvěryhodných aplikací, aby bylo zajištěno, že nebude narušen provoz serveru.

Cesta	Verze SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Server Microsoft Exchange

Při instalaci aplikace Kaspersky Endpoint Security na server Microsoft Exchange musíte vytvořit důvěryhodnou zónu z předdefinovaných výjimek a důvěryhodných aplikací, aby bylo zajištěno, že nebude narušen provoz serveru.

Předdefinované výjimky z kontroly

Cesta	Verze Microsoft Exchange
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016

	2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Předdefinované důvěryhodné aplikace

Cesta	Verze Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

Předdefinované výjimky z kontroly

Cesta	Verze System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Při instalaci aplikace Kaspersky Endpoint Security ve virtuálním prostředí Citrix musíte vytvořit důvěryhodnou zónu z předdefinovaných výjimek a důvěryhodných aplikací, aby bylo zajištěno, že nebude narušen provoz serveru.

Předdefinované výjimky z kontroly

Cesta
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt

%Temp%\Citrix\HDXRTConnector**.txt	
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt	\
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll	\
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll	\
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys	\
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll	\
*.vhd	F
*.avhd	F
*.vhdx	F
*.avhdx	F
*.pvp	F
*.lok	F
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)	F
%SystemRoot%\System32\drivers\CfsDep2.sys	F
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN	F
.vdiskcache	F
vdiskdif.vhdx	F
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb	S

Předdefinované důvěryhodné aplikace

Cesta	Řešení Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtual Apps and Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtual Apps and Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtual Apps and Desktops

%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtual Apps and Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace app
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace app

%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Při instalaci aplikace Kaspersky Endpoint Security ve virtuálním prostředí VMware musíte vytvořit důvěryhodnou zónu z předdefinovaných důvěryhodných aplikací, aby bylo zajištěno, že nebude narušen provoz serveru.

Předdefinované důvěryhodné aplikace

Cesta	Řešení VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon

C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

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.14.0\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.

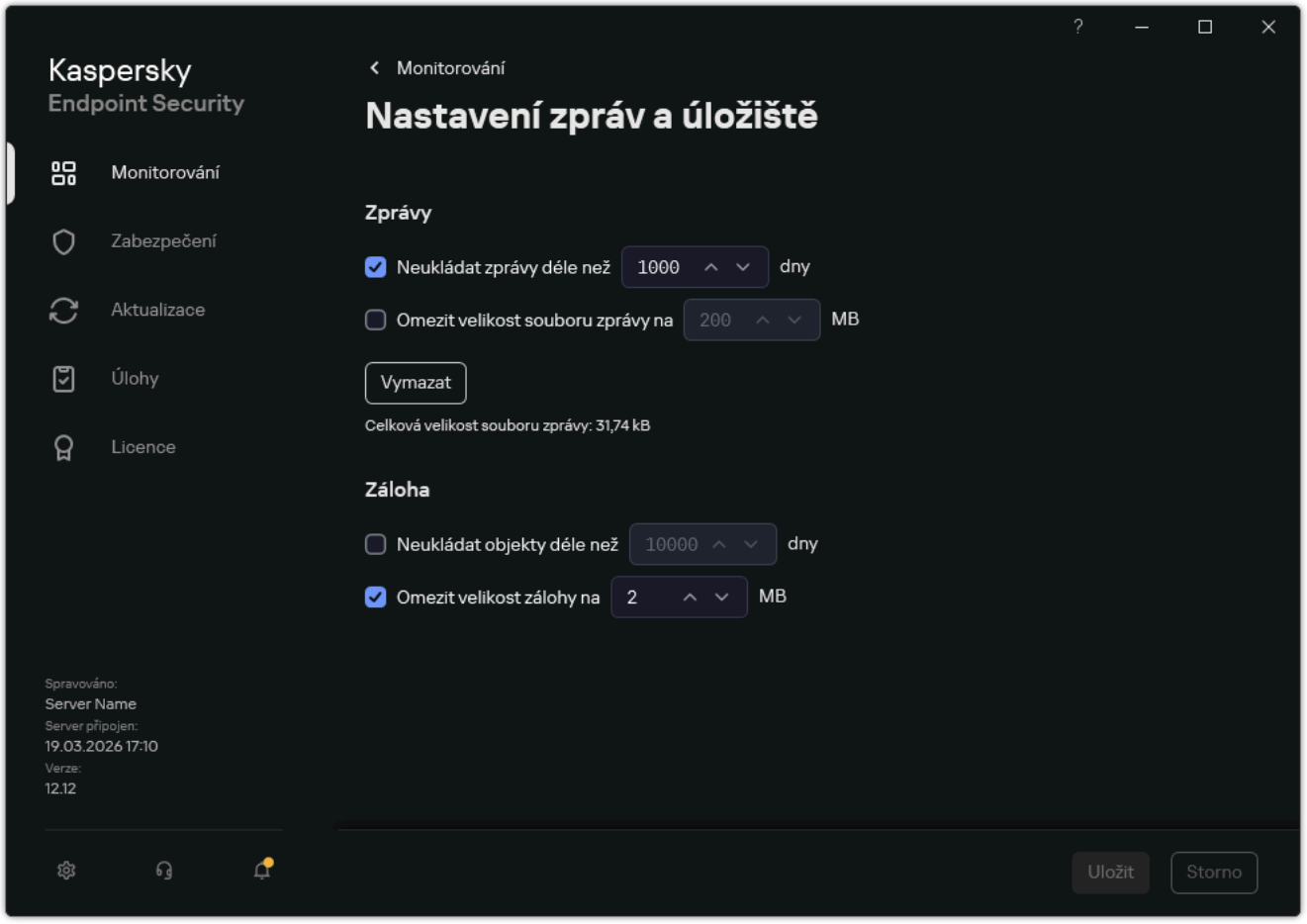
Konfigurace maximální doby uložení souborů v záloze

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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace v části **Obecná nastavení** klikněte na dlaždici **Zprávy a úložiště**.



Nastavení zálohy

3. Chcete-li omezit dobu uložení kopií souborů v záloze, zaškrtněte políčko **Neukládat objekty déle než N dní** v bloku **Záloha**. Zadejte maximální dobu uložení kopií souborů v záloze.

4. Uložte změny.

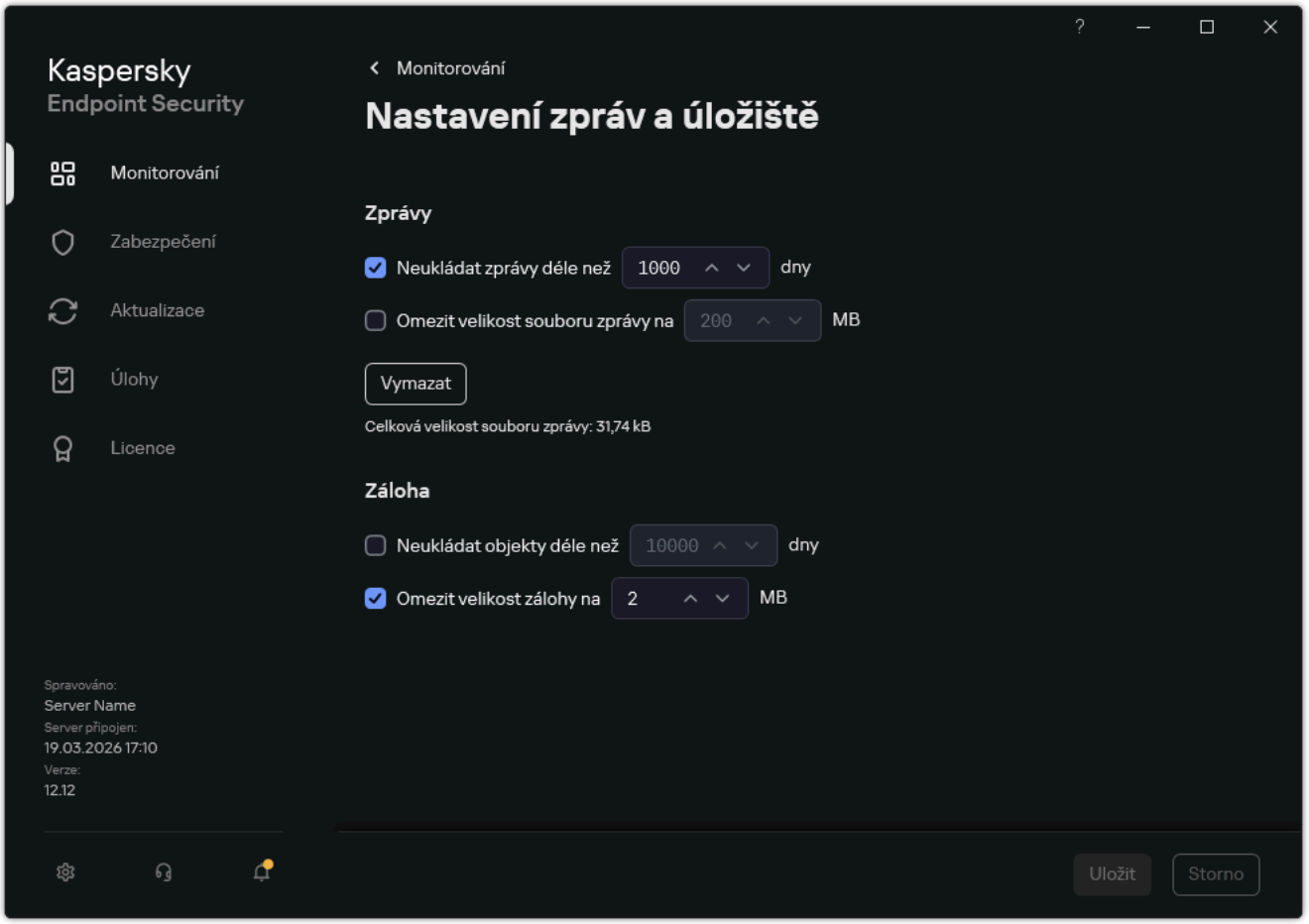
Konfigurace maximální velikosti zálohy

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.

Postup konfigurace maximální velikosti zálohy:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace v části **Obecná nastavení** klikněte na dlaždici **Zprávy a úložiště**.



Nastavení zálohy

3. V bloku **Záloha** zaškrtněte políčko **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 1024 MB. Aby nedošlo k překročení maximální velikosti úložiště, bude aplikace Kaspersky Endpoint Security po dosažení maximální velikosti úložiště automaticky z úložiště odstraňovat nejstarší soubory.

4. Uložte změny.

Obnovení souborů ze zálohy

Pokud je v souboru zjištěn škodlivý kód, aplikace Kaspersky Endpoint Security tento soubor zablokuje, přiřadí mu stav *Nedezinfikováno* a umístí jeho kopii do zálohy a pokusí se jej dezinfikovat. Pokud dezinfekce souboru proběhne úspěšně, stav záložní kopie souboru se změní na *Dezinfikován*. 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 *Dezinfikován* nebo *Odstraněno*. 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 (podrobnosti o obnovení aplikace ze služby Windows Store najdete v souborech nápovědy k systému Microsoft Windows).

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.

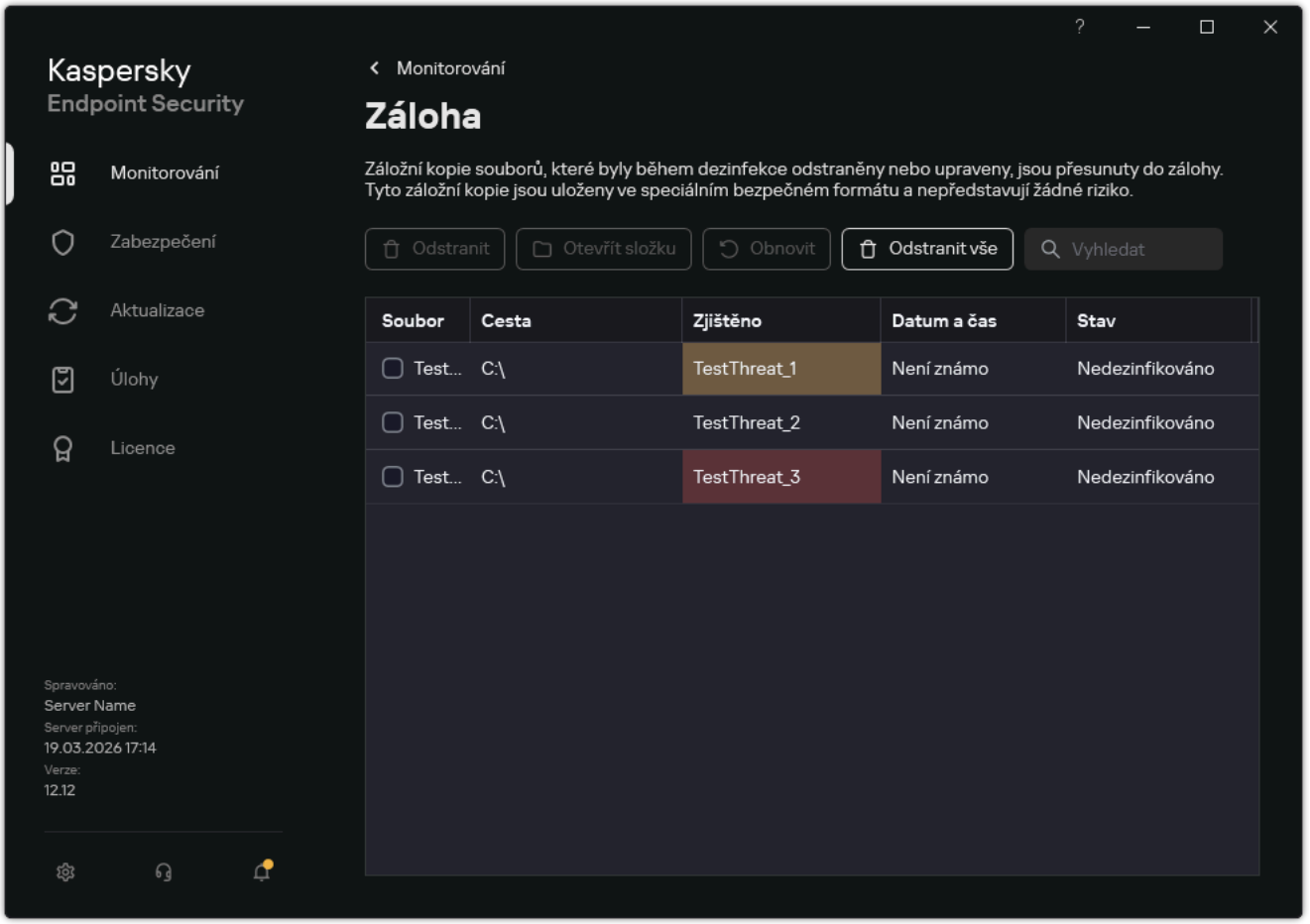
Pokud je do zálohy přesunuto několik souborů s identickými názvy a různým obsahem umístěných ve stejné složce, lze obnovit pouze poslední soubor umístěný do zálohy.

Postup obnovení souborů ze zálohy:

1. V hlavním okně aplikace v části **Monitorování** klikněte na dlaždici **Záloha**.

2. Tím otevřete seznam souborů v záloze; v tomto seznamu vyberte soubory, které chcete obnovit, a klikněte na **Obnovit**.

   Aplikace Kaspersky Endpoint Security obnoví z vybraných záložních kopií soubory v původních složkách.



Záloha

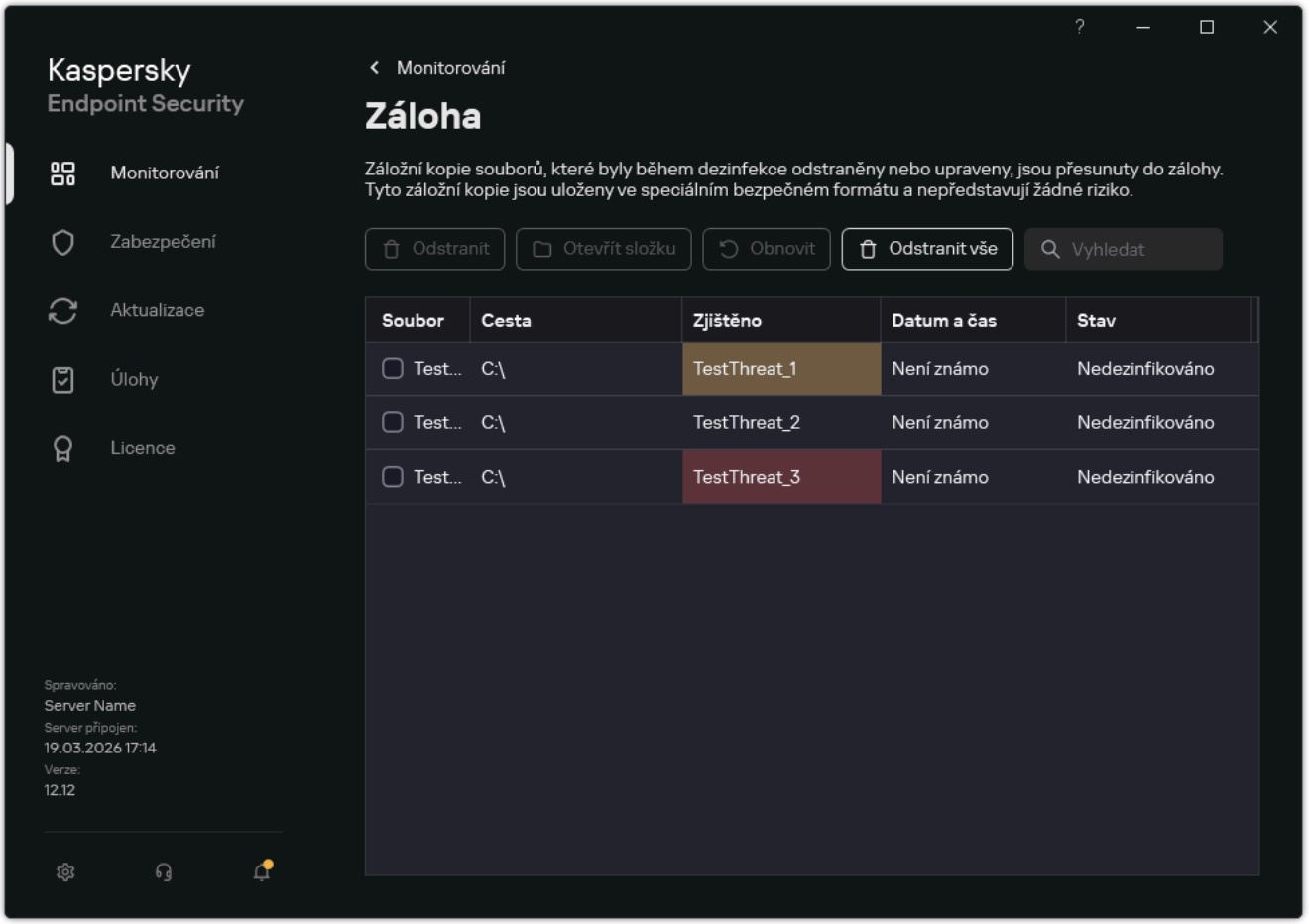
Odstranění záložních kopií souborů ze zálohy

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 v části **Monitorování** klikněte na dlaždici **Záloha**.
2. Tím otevřete seznam souborů v záloze; v tomto seznamu vyberte soubory, které chcete ze zálohy odstranit, a klikněte na **Odstranit**.

Aplikace Kaspersky Endpoint Security odstraní ze zálohy vybrané záložní kopie souborů.



Záloha

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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.
3. V bloku **Upozornění** klikněte na tlačítko **Konfigurovat 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**, jsou zobrazeny v protokolech aplikace. Události, jejichž políčka jsou zaškrtnuta ve sloupci **Uložit do protokolu událostí systému Windows**, jsou zobrazeny mezi protokoly systému Windows v kanálu `Application`.
6. Uložte změny.

Konfigurace zobrazení a doručování upozornění

Postup konfigurace zobrazení a doručování upozornění:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.
3. V bloku **Upozornění** klikněte na tlačítko **Konfigurovat 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 doručování upozornění.
5. Ve sloupci **Upozornit na obrazovce** zaškrtněte políčka vedle příslušných 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 příslušných 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 **Konfigurovat upozornění e-mailem**.

   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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.

3. V bloku **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.

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** 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 **Event selections** 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.

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.14.0\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 různých 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.

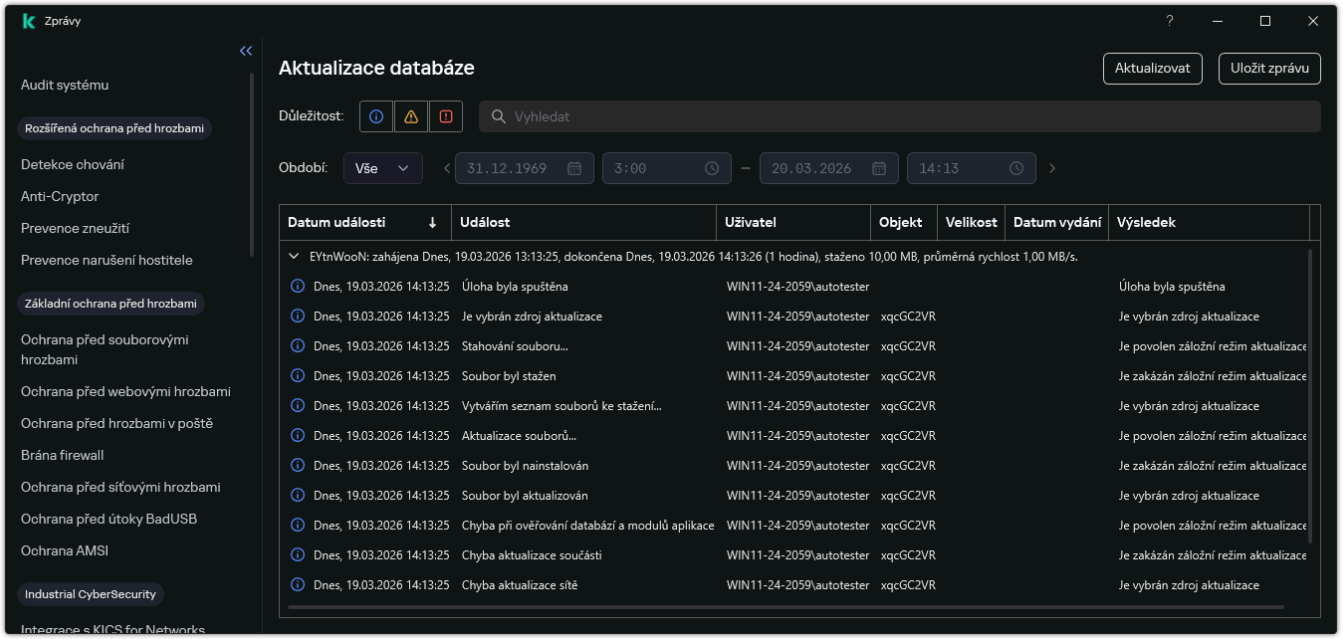
Pokud je aplikace Kaspersky Endpoint Security spuštěna pod správou aplikace Kaspersky Security Center, mohou být informace o událostech předávány na server pro správu Kaspersky Security Center (další podrobnosti naleznete v nápovědě k aplikaci Kaspersky Security Center).

Zobrazení sestav

Pokud uživatel může zobrazit zprávy, může zobrazit také všechny události zahrnuté ve zprávě.

Postup zobrazení zpráv:

1. V hlavním okně aplikace v části **Monitorování** klikněte na dlaždici **Zprávy**.



Zprávy

2. V seznamu součástí a úloh vyberte příslušnou 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.

3. Chcete-li zobrazit podrobné informace o události, vyberte událost ve zprávě.

V dolní části okna se zobrazí blok se shrnutím události.

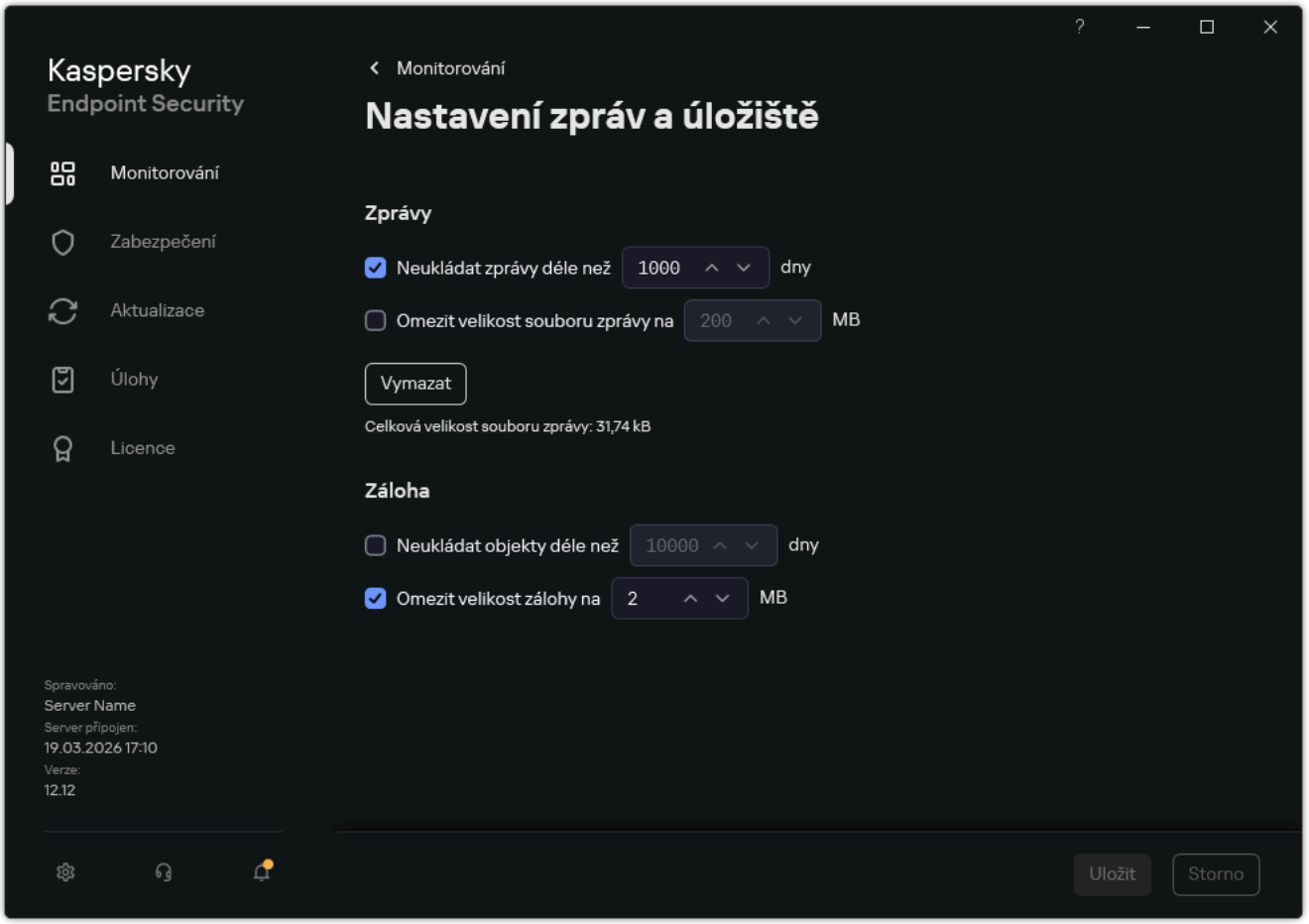
Konfigurace maximální doby uchovávání zpráv

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 hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace v části **Obecná nastavení** klikněte na dlaždici **Zprávy a úložiště**.



Nastavení zpráv

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.

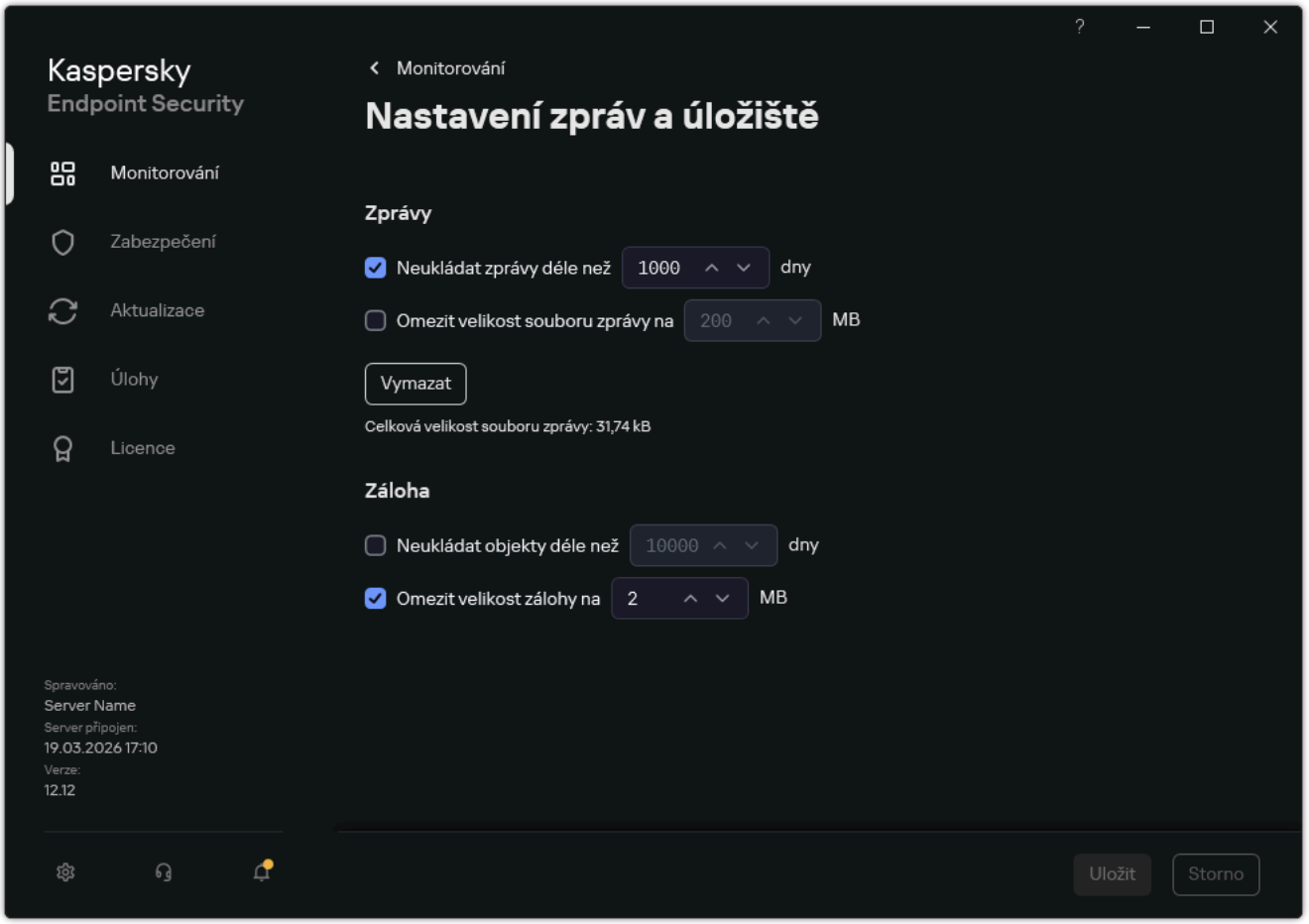
Konfigurace maximální velikosti souboru zprávy

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 hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace v části **Obecná nastavení** klikněte na dlaždici **Zprávy a úložiště**.



Nastavení zpráv

3. Pokud chcete omezit velikost souboru sestavy, v bloku **Zprávy** zaškrtněte políčko **Omezit velikost souboru zprávy na N MB**. Určete maximální velikost souboru zprávy.

4. Uložte změny.

Uložení zprávy do souboru

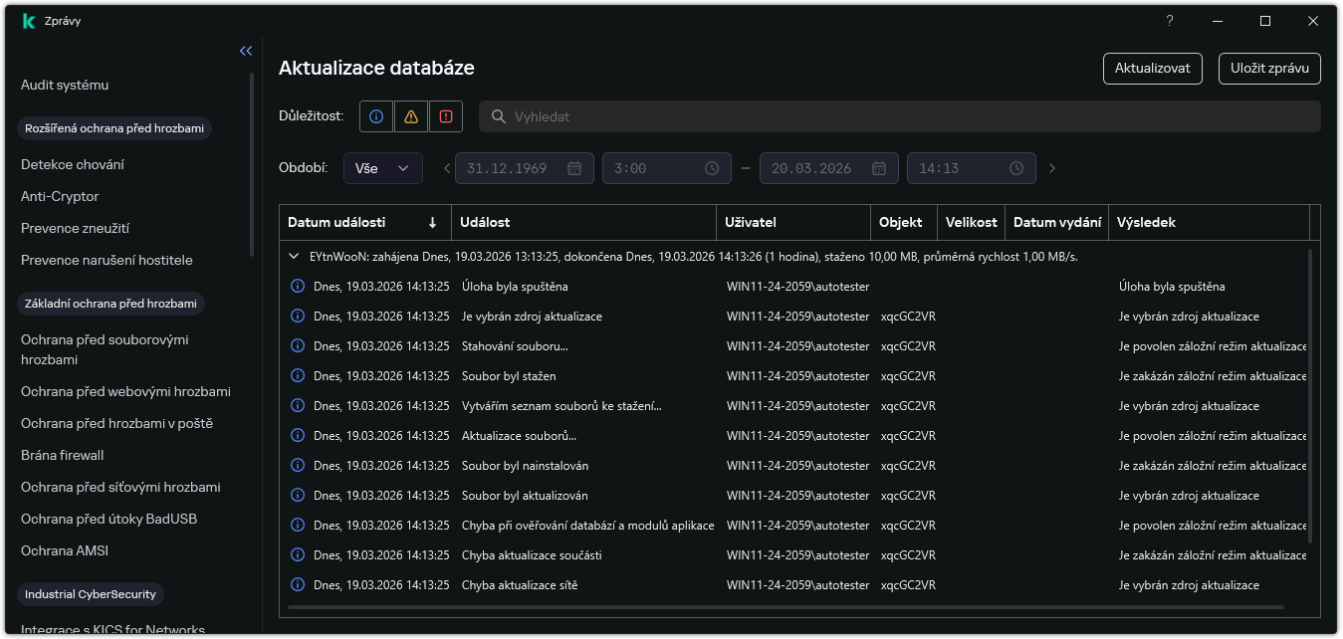
Uživatel je osobně odpovědný za zabezpečení informací ze zprávy uložených do souboru, a především za kontrolu těchto informací a omezení přístupu k nim.

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 v části **Monitorování** klikněte na dlaždici **Zprávy**.



Zprávy

2. Otevře se okno; v tomto okně 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. Zadejte název souboru zprávy.

7. Vyberte potřebný formát souboru zprávy: TXT nebo CSV.

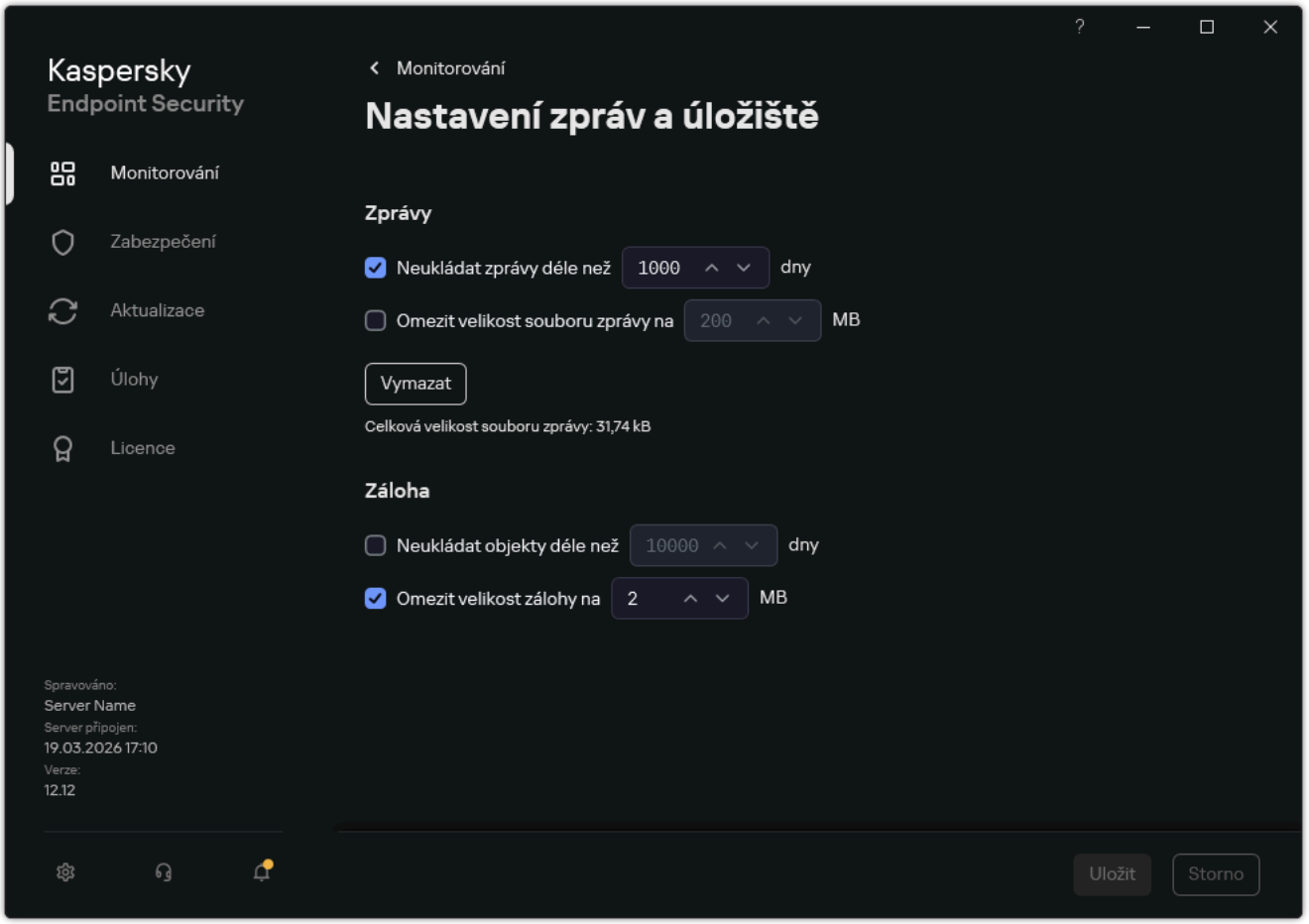
8. Uložte změny.

Mazání zpráv

Postup odebrání informací ze zpráv:

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace v části **Obecná nastavení** klikněte na dlaždici **Zprávy a úložiště**.



Nastavení zpráv

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 požadované 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

Sebeobrana brání jiným aplikacím provádět akce, které mohou narušovat provoz aplikace Kaspersky Endpoint Security a například odebrat aplikaci Kaspersky Endpoint Security z počítače. Sada dostupných technologií sebeobrany pro aplikaci Kaspersky Endpoint Security závisí na tom, zda je systém 32bitový, nebo 64bitový (viz tabulka níže). Sebeobrana také zahrnuje ochranu heslem a ochranu připojení k serveru pro správu.

Ochrana heslem umožňuje omezit přístup uživatelů k aplikaci Kaspersky Endpoint Security podle oprávnění, která jsou jim udělena (například oprávnění k ukončení aplikace).

Ochrana připojení k serveru pro správu zabraňuje neoprávněnému opětovnému připojení počítače k nedůvěryhodnému serveru.

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 a další soubory aplikace; • 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 brání jiným aplikacím (například TeamViewer nebo RemotelyAnywhere) získat přístup k aplikaci Kaspersky Endpoint Security.	✓	– (kromě Windows 7)

Povolení a zakázání sebeobrany

Aplikace Kaspersky Endpoint Security brání úpravám nebo odstranění souborů aplikace na pevném disku, paměťových procesů a záznamů v systémovém registru.

Tato technologie blokuje přístup k následujícím součástem aplikace:

- soubory v instalační složce aplikace Kaspersky Endpoint Security a další soubory aplikace;
- klíče registru se záznamy patřícími aplikaci;
- procesy spuštěné aplikací.

Mechanismus sebeobrany aplikace Kaspersky Endpoint Security je ve výchozím nastavení povolen.

Jak povolit nebo zakázat součást Sebeobrana v konzole pro správu (MMC)

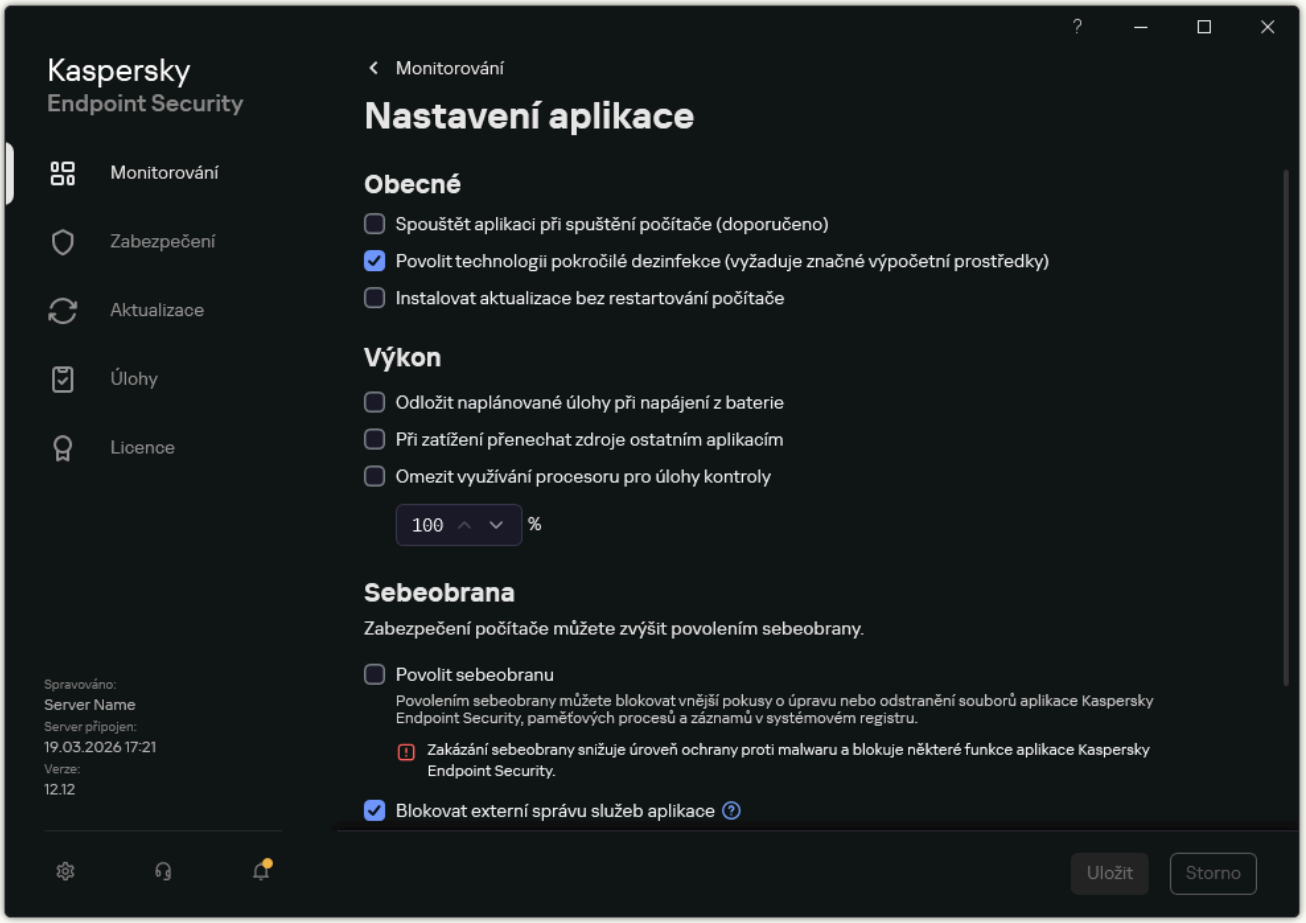
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. Pomocí zaškrtávacího políčka **Povolit sebeobranu** aktivujte nebo deaktivujte mechanismus sebeobrany.
5. Uložte změny.

Jak povolit nebo zakázat součást Sebeobrana ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Self-Defense**.
5. Pomocí přepínače **Self-Defense ENABLED** povolte nebo zakažte mechanismus sebeobrany.
6. Uložte změny.

Jak povolit nebo zakázat součást Sebeobrana v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

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.

Používejte technologii AM-PPL nepřetržitě. AM-PPL je důležitou součástí ochrany operačního systému. Zakázání podpory AM-PPL může způsobit selhání některých funkcí aplikace Kaspersky Endpoint Security (například integrace aplikace s aplikací Windows Security Center). Zakázání podpory AM-PPL je povoleno pouze v samostatném testovacím prostředí pro účely odstraňování problémů.

Technologie 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.

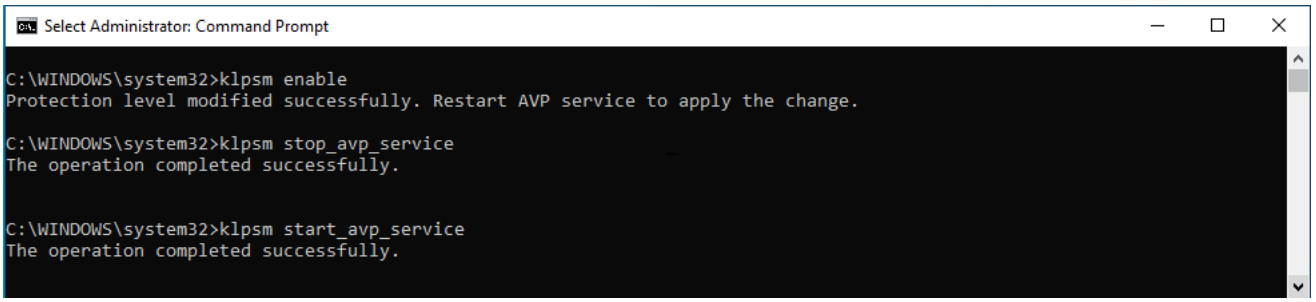
3. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

   Cestu ke spustitelnému souboru můžete přidat do systémové proměnné %PATH% během instalace aplikace.

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

Ochrana služeb aplikace před externí správou

Ochrana služeb aplikace před externí správou blokuje pokusy uživatelů a jiných aplikací zastavit služby aplikace Kaspersky Endpoint Security. Ochrana zajišťuje provoz následujících služeb:

- Služba Kaspersky Endpoint Security (AVP.KES.14.0)
- Služba Kaspersky Seamless Update Service (AVPSUS.KES.14.0)

Chcete-li aplikaci ukončovat z příkazového řádku, zakažte ochranu služeb Kaspersky Endpoint Security před externí správou.

Externí správu služeb aplikace můžete povolit pouze v počítačích, které nepodporují technologii AM-PPL, nebo v počítačích, které mají tuto technologii zakázánu.

Jak povolit nebo zakázat ochranu služeb aplikace před externí správou v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. Pomocí zaškrtávacího políčka **Blokovat externí správu služeb aplikace** povolíte nebo zakážete ochranu služeb Kaspersky Endpoint Security před externí správou.
5. Uložte změny.

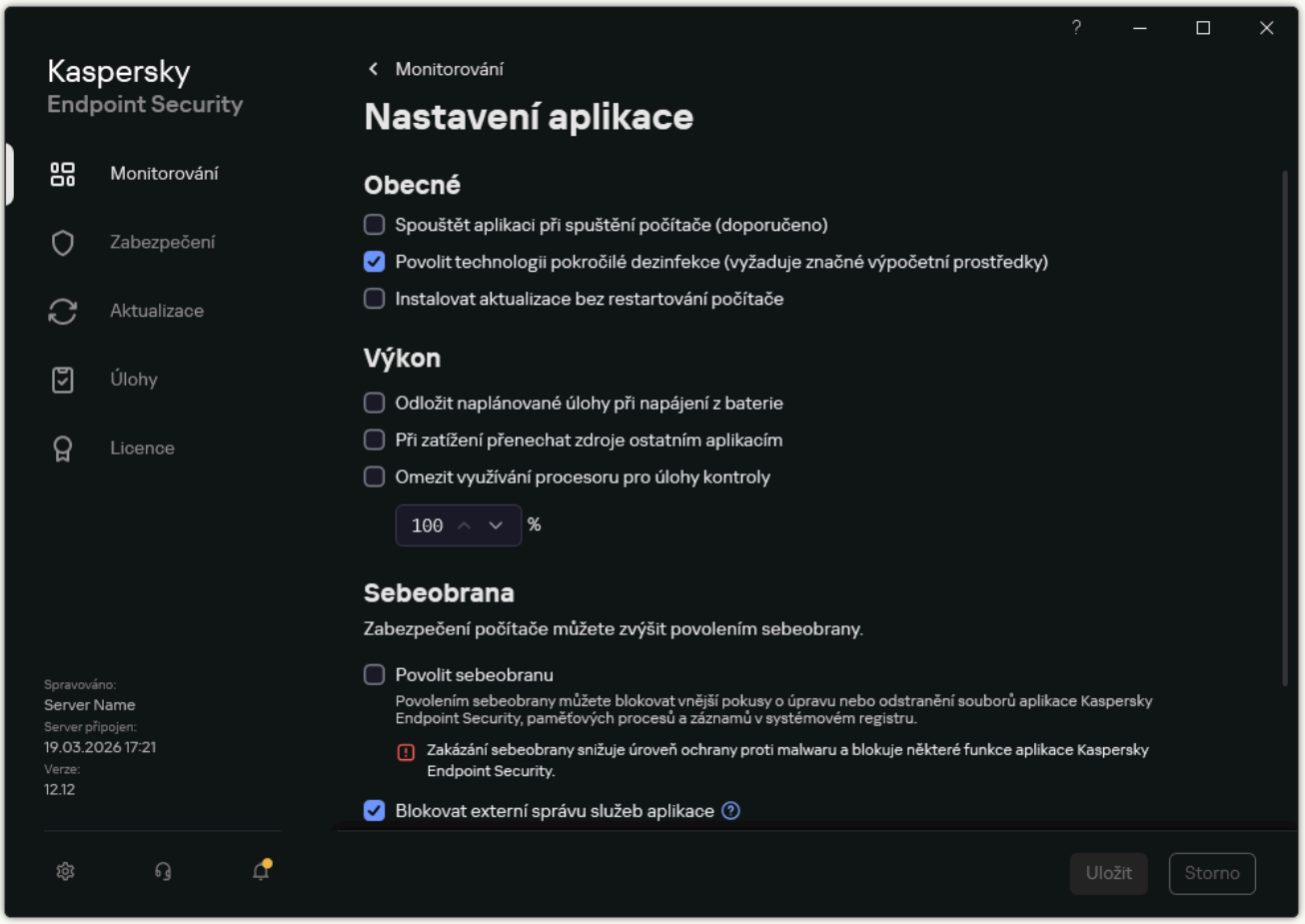
Jak povolit nebo zakázat ochranu služeb aplikace před externí správou ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Self-Defense**.
5. Pomocí zaškrtávacího políčka **Block external management of application services** povolíte nebo zakážete ochranu služeb Kaspersky Endpoint Security před externí správou.
6. Uložte změny.

Jak povolit nebo zakázat ochranu služeb aplikace před externí správou v rozhraní aplikace

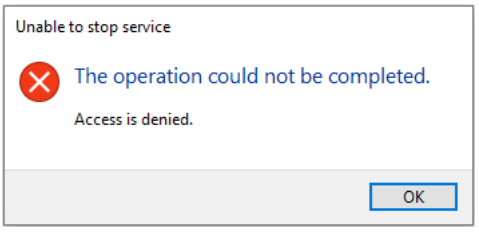
1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

3. Pomocí zaškrtávacího políčka **Blokovat externí správu služeb aplikace** povolíte nebo zakážete ochranu služeb Kaspersky Endpoint Security před externí správou.
4. Uložte změny.

Výsledkem je, že když se uživatel pokusí zastavit služby aplikace, zobrazí se systémové okno s chybovou zprávou. Uživatel může spravovat služby aplikace pouze z rozhraní aplikace Kaspersky Endpoint Security.



Chyba přístupu ke službám aplikace

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 hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Výjimky a typy zjištěných objektů**.
3. V bloku **Výjimky** klikněte na odkaz **Zadat důvěryhodné aplikace**.

4. V okně, které se otevře, klikněte na tlačítko **Přidat**.
5. Vyberte spustitelný soubor aplikace pro vzdálenou správu.

   Cestu můžete rovněž zadat ručně. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
6. Zaškrtněte políčko **Povolit interakci s rozhraním aplikace Kaspersky Endpoint Security**.
7. Uložte změny.

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:

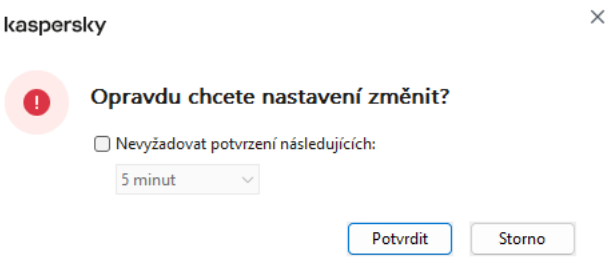
- Zadejte uživatelské jméno a heslo.

  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 nebo účet přidaný ručně.
- 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).

V okně pro zadání hesla můžete přepínat jazyky pouze stisknutím **ALT+SHIFT**. Používání jiných zkratek, i když jsou nakonfigurovány v operačním systému, nefunguje při přepínání jazyků.



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, měli byste zadat přístupové údaje k účtu. Ochrana heslem podporuje následující účty:

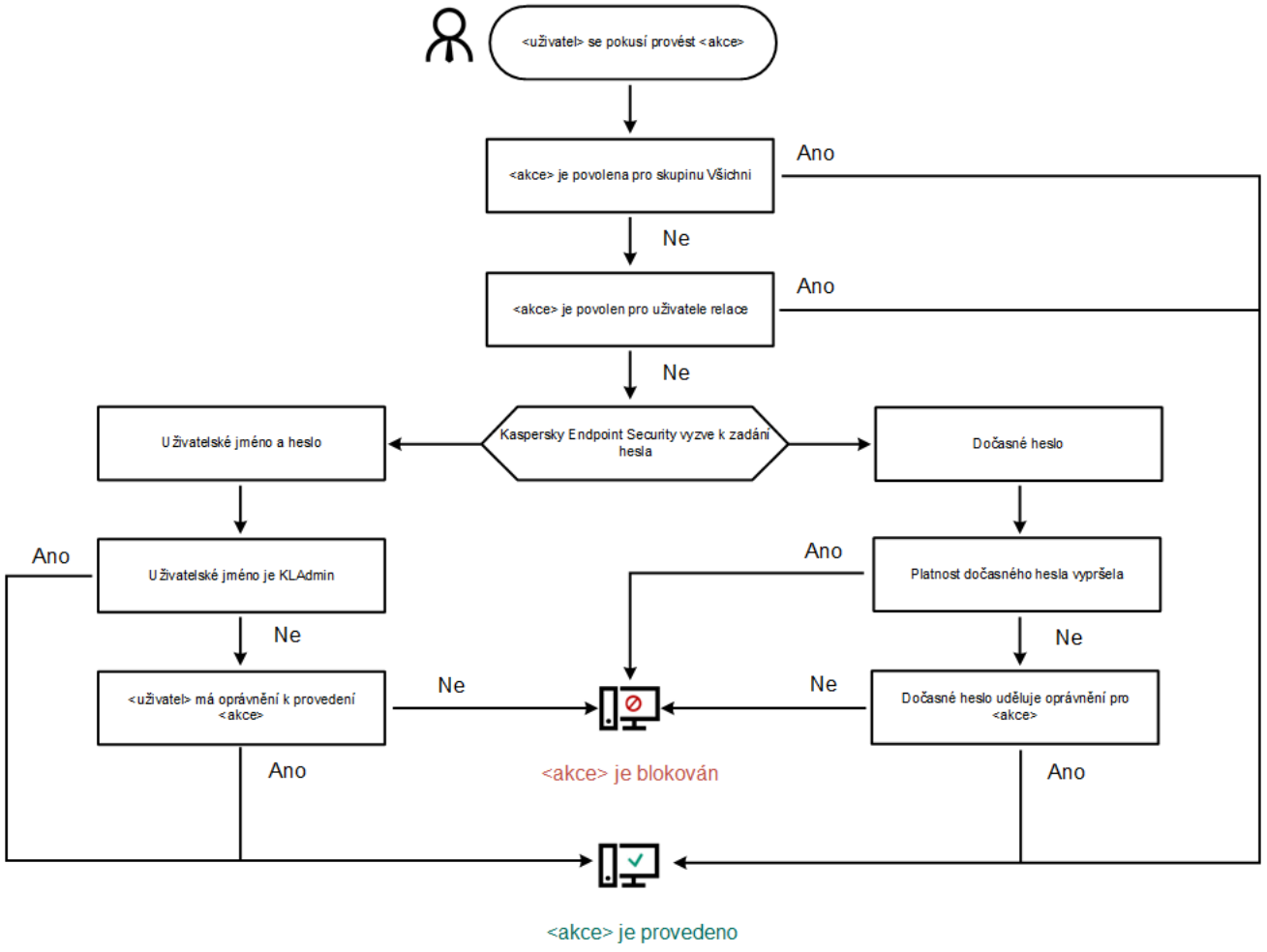
- **KLAdmin**. Účet správce s neomezeným přístupem k aplikaci Kaspersky Endpoint Security. Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem. Oprávnění k účtu KLAdmin nelze odvolat. Když povolíte ochranu heslem, aplikace Kaspersky Endpoint Security vás vyzve k nastavení hesla k účtu KLAdmin.
- **Účet byl přidán ručně**. Účet mimo doménu Active Directory. Tento účet služby můžete použít místo účtu KLAdmin, pokud nechcete sdílet heslo správce. Můžete nastavit jakékoli uživatelské jméno a heslo a nakonfigurovat individuální oprávnění.
- **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).

Jak povolit ochranu heslem v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Rozhraní**.
4. V bloku **Ochrana heslem** klikněte na tlačítko **Nastavení**.
   Otevře se okno s nastavením ochrany heslem.
5. Pomocí zaškrtávacího políčka **Povolit ochranu heslem** můžete tuto součást povolit nebo zakázat.
6. V části **Oprávnění** vyberte účet KLAdmin.
7. Tím se otevře okno; v tomto okně klikněte na možnost **Heslo** a nastavte heslo pro účet KLAdmin.
   Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem.

Pokud jste zapomněli heslo ke svému účtu KLAdmin, můžete jej resetovat ve vlastnostech zásady.

8. Vraťte se na seznam účtů.
9. Nastavení oprávnění pro všechny uživatele v podnikové síti:
   a. V části **Oprávnění** vyberte skupinu Všichni.
      Skupina uživatelů Všichni je integrovaná skupina systému Windows, která zahrnuje všechny uživatele v podnikové síti.
   b. V okně, které se otevřelo, 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.
10. Uložte změny.

Jak povolit ochranu heslem ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Self-Defense**.
5. V části **Password Protection** pomocí přepínače **Password Protection ENABLED** můžete tuto součást povolit nebo zakázat.
6. Zadejte heslo k účtu KLAdmin a potvrďte jej.
   Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem.

   Pokud jste zapomněli heslo ke svému účtu KLAdmin, můžete jej resetovat ve vlastnostech zásady.
7. Vraťte se na seznam účtů.
8. Nastavení oprávnění pro všechny uživatele v podnikové síti:
   a. V tabulce účtů vyberte skupinu Všichni.
      Skupina uživatelů Všichni je integrovaná skupina systému Windows, která zahrnuje všechny uživatele v podnikové síti.
   b. V okně, které se otevřelo, 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 **Exit the application**, 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.
9. Uložte změny.

Jak povolit ochranu heslem v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.

3. Pomocí přepínače **Ochrana heslem** můžete tuto součást povolit nebo zakázat.

4. 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.

5. Nastavení oprávnění pro všechny uživatele v podnikové síti:

   a. V tabulce účtu 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.

6. 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

Ochrana heslem umožňuje udělit aplikaci Kaspersky Endpoint Security přístup k jednotlivým uživatelským účtům služby Active Directory a ručně přidaným uživatelským účtům.

Uživatelské účty služby Active Directory

Aplikaci Kaspersky Endpoint Security můžete udělit přístup k jednotlivým uživatelům nebo skupinám v rámci domény Active Directory. 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.

Uživatelské účty přidané ručně

Můžete vytvořit uživatelský účet, který se nenachází ve službě Active Directory, a přiřadit mu individuální oprávnění. To znamená, že můžete vytvořit *uživatelský účet služby* a používat jej místo účtu KLAdmin. Nemusíte tak sdílet heslo KLAdmin s ostatními uživateli ani vytvářet nové účty služby Active Directory. Zadat můžete jakékoli uživatelské jméno a heslo. Uživatelskému účtu služby můžete například udělit oprávnění **Zobrazit zprávy**. Pokud má například skupina „Všichni" zakázáno zobrazování zpráv, můžete sestavy otevírat pomocí uživatelského účtu služby nebo uživatelského účtu KLAdmin.

Udělení oprávnění jednotlivým uživatelům nebo skupinám

Jak udělit oprávnění jednotlivým uživatelům nebo skupinám v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Rozhraní**.
4. V bloku **Ochrana heslem** klikněte na tlačítko **Nastavení**.

   Otevře se okno s nastavením ochrany heslem.
5. V tabulce účtu klikněte na **Přidat**.
6. Vyberte typ uživatelského účtu, který chcete přidat:

   - **Vybrat uživatele/skupinu z Active Directory** – Uživatelské účty služby Active Directory.

     Uživatelský účet vyberete kliknutím na možnost **Vybrat**. Vyberte uživatele nebo skupinu ve službě Active Directory a potvrďte výběr.
   - **Přidat uživatele / skupinu uživatelů ručně** pro ručně přidaný uživatelský účet služby.

     Pokud chcete přidat uživatelský účet služby, zadejte uživatelské jméno a heslo (například SecureAdmin).

     > Heslo uživatelského účtu služby můžete resetovat v nastavení zásad. Heslo uživatelského účtu služby je třeba resetovat stejným způsobem jako heslo účtu KL Admin. Pokud je povolena úprava nastavení ochrany heslem („zámek" je otevřený) nebo se v počítači nepoužívá žádná zásada, můžete v rozhraní aplikace resetovat heslo účtu uživatele služby. Za tímto účelem potvrďte změny údajů o účtu uživatele služby pomocí hesla KL Admin.
7. V seznamu **Oprávnění** 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 KL Admin 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.
8. Uložte změny.

Jak udělit oprávnění jednotlivým uživatelům nebo skupinám ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Self-Defense**.
5. V bloku **Password Protection** klikněte na odkaz **User permissions**.

   Otevře se formulář pro udělení oprávnění pro povolení hesla.
6. Klikněte na tlačítko **Add**.
7. Vyberte typ uživatelského účtu, který chcete přidat:

   - **Select from Active Directory** – Uživatelské účty služby Active Directory.

     Uživatelský účet vyberete kliknutím na možnost **Edit**. Vyberte uživatele nebo skupinu ve službě Active Directory a potvrďte výběr.
   - **Add manually** pro ručně přidaný uživatelský účet služby.

     Pokud chcete přidat uživatelský účet služby, zadejte uživatelské jméno a heslo (například SecureAdmin).

     > Heslo uživatelského účtu služby můžete resetovat v nastavení zásad. Heslo uživatelského účtu služby je třeba resetovat stejným způsobem jako heslo účtu KL Admin. Pokud je povolena úprava nastavení ochrany heslem („zámek" je otevřený) nebo se v počítači nepoužívá žádná zásada, můžete v rozhraní aplikace resetovat heslo účtu uživatele služby. Za tímto účelem potvrďte změny údajů o účtu uživatele služby pomocí hesla KL Admin.
8. V seznamu **Permissions** 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 **Exit the application**, 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.

9. Klikněte na tlačítko **Add**.
10. Uložte změny.

Jak udělit oprávnění jednotlivým uživatelům nebo skupinám v uživatelském rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Rozhraní**.
3. V tabulce účtu klikněte na **Přidat**.
4. Vyberte typ uživatelského účtu, který chcete přidat:
   - **Vybrat uživatele/skupinu z Active Directory** – Uživatelské účty služby Active Directory.

     Uživatelský účet vyberete kliknutím na možnost **Vyberte uživatele nebo skupinu**. Vyberte uživatele nebo skupinu ve službě Active Directory a potvrďte výběr.
   - **Přidat uživatele ručně** pro ručně přidaný uživatelský účet služby.

     Pokud chcete přidat uživatelský účet služby, zadejte uživatelské jméno a heslo (například SecureAdmin).

     Heslo uživatelského účtu služby můžete resetovat v nastavení zásad. Heslo uživatelského účtu služby je třeba resetovat stejným způsobem jako heslo účtu KLAdmin. Pokud je povolena úprava nastavení ochrany heslem („zámek" je otevřený) nebo se v počítači nepoužívá žádná zásada, můžete v rozhraní aplikace resetovat heslo účtu uživatele služby. Za tímto účelem potvrďte změny údajů o účtu uživatele služby pomocí hesla KLAdmin.
5. V seznamu **Oprávnění** 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.

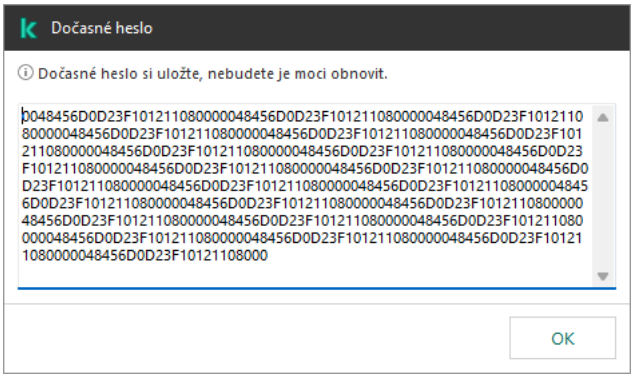
Jak povolit uživateli provést blokovanou akci pomocí dočasného hesla prostřednictvím konzoly pro správu (MMC)

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 **Applications**.
6. V seznamu aplikací společnosti Kaspersky, které jsou nainstalovány v počítači, vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** a dvojitým kliknutím otevřete vlastnosti aplikace.
7. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Rozhraní**.
8. V bloku **Ochrana heslem** klikněte na tlačítko **Nastavení**.
9. V okně, které se otevře, v bloku **Dočasné heslo** klikněte na tlačítko **Seznam dočasných hesel**.
   Otevře se okno Správa dočasných hesel.
10. Klikněte na tlačítko **Přidat**.
11. V poli **Datum vypršení platnosti** zadejte datum vypršení platnosti dočasného hesla.
12. V tabulce **Rozsah dočasného hesla** zaškrtněte políčka vedle akcí, které bude mít uživatel k dispozici po zadání dočasného hesla.
13. Klikněte na tlačítko **Vytvořit**.
    Otevře se okno obsahující dočasné heslo (viz obrázek níže).
14. Zkopírujte heslo a poskytněte jej uživateli.

Jak povolit uživateli provést blokovanou akci pomocí dočasného hesla prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Assets (Devices)**.
2. Klikněte na název počítače, u něhož chcete uživateli povolit provedení blokované akce.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. V okně nastavení aplikace vyberte možnost **General settings → Interface**.
7. V bloku **Temporary passwords** klikněte na tlačítko **Add**.
8. V poli **Datum vypršení platnosti** zadejte datum vypršení platnosti dočasného hesla.
9. V tabulce **Rozsah dočasného hesla** zaškrtněte políčka vedle akcí, které bude mít uživatel k dispozici po zadání dočasného hesla.
10. Klikněte na tlačítko **Vytvořit**.
    Otevře se okno obsahující dočasné heslo.
11. Zkopírujte heslo a poskytněte jej uživateli.

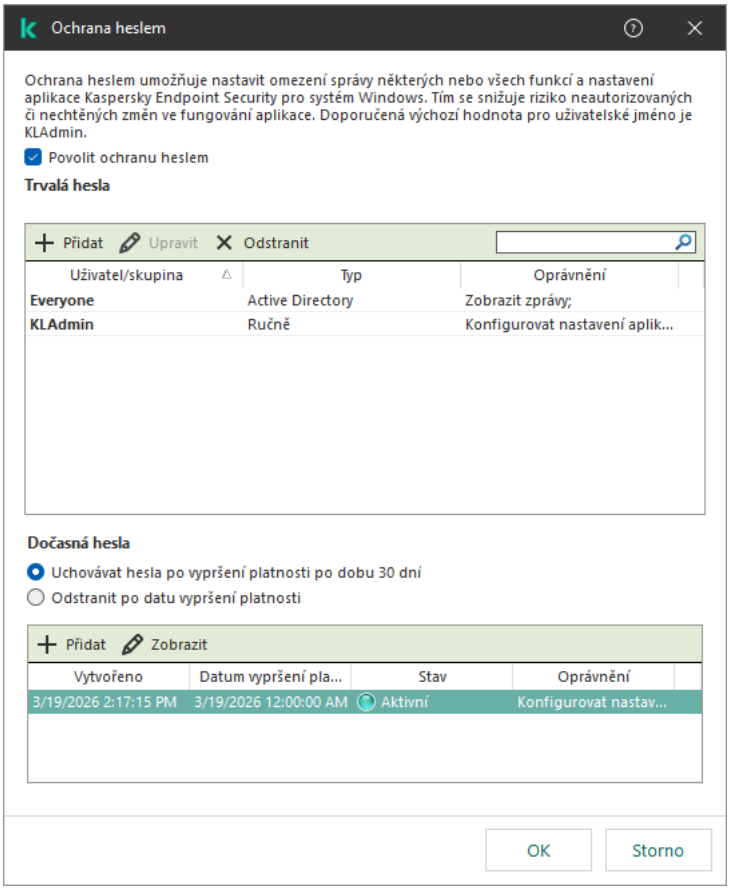


Dočasné heslo

Rušení dočasného hesla

Od verze 12.9 zahrnuje aplikace Kaspersky Endpoint Security pro systém Windows zahrnuje funkci *Správa dočasných hesel*. Správa dočasných hesel umožňuje provádět následující akce:

- Uložit historii hesel (až 30 dní).
- Sledovat stav dočasného hesla: *Aktivní*, *Vypršela platnost*, *Odvolané*.
- Odvolávat dočasná hesla.



Správa dočasných hesel

Správa dočasných hesel aktualizuje stav hesla a odpojí heslo až po synchronizaci počítače s aplikací Kaspersky Security Center.

Jak odvolat dočasné heslo Light Agent 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 **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 (14.0)** a dvojitým kliknutím otevřete vlastnosti aplikace.
7. V okně nastavení aplikace vyberte možnost **Obecná nastavení → Rozhraní**.
8. V bloku **Ochrana heslem** klikněte na tlačítko **Nastavení**.
9. Otevře se okno; v tom okně v části **Dočasné heslo** nakonfigurujte nastavení úložiště pro hesla, kterým vypršela platnost.
10. Klikněte na tlačítko **Seznam dočasných hesel**.
    Otevře se okno Správa dočasných hesel. Správa dočasných hesel zobrazuje datum vypršení platnosti hesla, stav hesla a seznam oprávnění.
11. Vyberte aktivní dočasné heslo, které chcete odvolat, a dvojitým kliknutím na něj otevřete jeho vlastnosti.
12. V okně, které se otevře, klikněte na tlačítko **Odvolat**.
13. Uložte změny. Chcete-li zásady použít v počítačích, zavřete zámky.

[Jak odvolat dočasné heslo ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Klikněte na název počítače, u něhož chcete uživateli povolit provedení blokované akce.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. V okně nastavení aplikace vyberte možnost **General settings** → **Interface**.
7. V části **Temporary passwords** nakonfigurujte úložiště hesel, jejichž platnost vypršela.
8. Klikněte na odkaz **Temporary password**.
   Otevře se okno Správa dočasných hesel. Správa dočasných hesel zobrazuje datum vypršení platnosti hesla, stav hesla a seznam oprávnění.
9. Vyberte aktivní dočasné heslo, které chcete odpojit.
10. V okně, které se otevře, klikněte na tlačítko **Revoke password**.
11. Uložte změny. Chcete-li zásady použít v počítačích, zavřete zámky.

Správa dočasných hesel tak nastaví stav hesla na *Odpojování (synchronizace s hostitelem)*. Po synchronizaci počítače s aplikací Kaspersky Security Center aplikace odvolá dočasné heslo a okamžitě zablokuje udělená oprávnění.

Zvláštní aspekty oprávnění týkajících se ochrany heslem

Oprávnění týkající se ochrany heslem mají některé důležité aspekty a omezení, které je třeba zvážit.

Konfigurace 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 kontroly jiným uživatelům než KL Admin, 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 **Konfigurace nastavení aplikace**.
- Aby bylo možné zakázat součásti ochrany z místní nabídky (pomocí položky nabídky **Pozastavit ochranu**), uživatel musí mít kromě oprávnění **Zakázat součásti kontroly** také oprávnění **Zakázat součásti ochrany**.

Zakázat součásti kontroly

- Není možné udělit oprávnění k deaktivaci součástí kontroly pro skupinu Všichni. Chcete-li povolit zakazování součástí kontroly jiným uživatelům než KL Admin, 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 **Konfigurace nastavení aplikace**.
- Aby bylo možné zakázat součásti kontroly z místní nabídky (pomocí položky nabídky **Pozastavit ochranu**), uživatel musí mít kromě oprávnění **Zakázat součásti ochrany** také oprávnění **Zakázat součásti kontroly**.

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 šifrovaném disku

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.

Zobrazit zprávy

Neexistují žádné zvláštní požadavky nebo omezení.

Obnovit ze zálohy

Neexistují žádné zvláštní požadavky nebo omezení.

Export nastavení

Ve výchozím nastavení je export nastavení aplikace do skupiny Všichni zakázán. Nastavení aplikace můžete exportovat pomocí uživatelského účtu KLAdmin. Export nastavení aplikace zahrnuje pouze vytvoření konfiguračního souboru s nastavením aplikace Kaspersky Endpoint Security v rozhraní aplikace. Oprávnění neomezuje export seznamů výjimek z kontroly, důvěryhodných webových adres, důvěryhodných zařízení ani jiných seznamů vedených součástmi aplikace.

Resetování hesla KLAdmin

Pokud jste zapomněli heslo ke svému účtu KLAdmin, můžete jej resetovat ve vlastnostech zásady. V rozhraní aplikace heslo resetovat nelze.

Akce chráněné heslem můžete provádět pomocí dočasného hesla. V takovém případě nemusíte zadávat přihlašovací údaje k účtu KLAdmin.

Pokud počítač není připojen k aplikaci Kaspersky Security Center a zapomněli jste heslo k účtu KLAdmin, heslo není možné obnovit.

Jak resetovat heslo k účtu KLAdmin pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Rozhraní**.
4. V bloku **Ochrana heslem** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, zrušte zaškrtnutí políčka **Povolit ochranu heslem**.
6. Uložte změny.
7. Znovu zaškrtněte políčko **Povolit ochranu heslem**.
8. Klikněte na tlačítko **OK**.
   Tím se otevře okno s heslem správce.
9. Zadejte nové heslo k účtu KLAdmin a potvrďte jej.
10. Uložte změny.

[Jak resetovat heslo k účtu KLAdmin ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. Přejděte na **General Settings** → **Self-Defense**.
7. V části **Ochrana heslem** vypněte přepínač **Ochrana heslem**.
8. Uložte změny.
9. Znovu zapněte přepínač **Ochrana heslem**.
10. Zadejte nové heslo k účtu KLAdmin a potvrďte jej.
11. Uložte změny.

V důsledku toho se heslo k vašemu účtu KLAdmin po použití zásady aktualizuje.

Ochrana připojení k serveru pro správu

Počítač se k serveru pro správu připojuje pomocí součásti *Network Agent* aplikace Kaspersky Security Center. Pokud má útočník dostatečná práva k úpravě nastavení připojení k serveru, hrozí riziko připojení počítače k nedůvěryhodnému serveru. To by útočníkovi umožnilo použít vlastní zásady skupiny a například zakázat sebeobranu aplikace. Kaspersky Endpoint Security může neoprávněnému opětovnému připojení počítače k jinému serveru zabránit. Pro ochranu připojení k serveru aplikace doporučuje nastavit heslo a používat funkci Password-Based key Derivation Function (PBKDF2). Přístup do aplikace bez hesla je proto nemožný.

Chcete-li zajistit komplexní ochranu aplikace Kaspersky Endpoint Security a součásti Network Agent před neoprávněným přístupem, doporučujeme povolit další ochranu. U aplikace Kaspersky Endpoint Security doporučujeme povolit Ochranu heslem. Pro ochranu součásti Network Agent doporučujeme nastavit heslo k odinstalaci. Podrobnosti o ochraně před odebráním součásti Network Agent najdete v nápovědě k aplikaci Kaspersky Security Center .

Připojení počítače k serveru pro správu se spravuje pomocí úlohy *Ochrana připojení k serveru pro správu*. Tato úloha umožňuje provádět následující akce:

- Nastavit heslo na ochranu připojení k serveru.
- Změnit heslo.
- Znovu připojit počítač k jinému serveru.
- Zakázat ochranu připojení k serveru.

Ověření počítače při připojování k serveru pro správu

Po nastavení hesla aplikace vytvoří datové pole transformací hesla funkcí PBKDF2. Aplikace poté toto datové pole zašifruje pomocí klíče součásti Network Agent. Aplikace pomocí tohoto šifrovaného datového pole u následných připojeních kontroluje práva a oprávnění serveru pro správu.

Následně při každém pokusu o opětovné připojení počítače k serveru pro správu aplikace dešifruje datové pole pomocí klíče součásti Network Agent a porovná je s místní kopií. Pokud se neshodují, je přístup k aplikaci omezen.

Ochrana připojení k serveru pro správu

[Jak nastavit heslo pro ochranu připojení k serveru v konzole pro správu (MMC)]

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Ochrana připojení k serveru pro správu**.

Krok 2. Ochrana připojení k serveru pro správu

Nastavení hesla na ochranu připojení k serveru pro správu:

1. V části **Ochrana připojení k serveru pro správu** vyberte možnost **Chránit heslem**.
2. V rozevíracím seznamu **Server pro správu** vyberte možnost **Nový server**.
3. V poli **Heslo pro připojení k serveru pro správu** nastavte heslo pro připojení k serveru pro správu a potvrďte je.

   Pokud heslo zapomenete, můžete si je změnit pomocí úlohy.
4. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.7 nebo dřívější verzi aplikace, zaškrtněte políčko **Povolit kompatibilitu šifrování hesel pro předchozí verze aplikace (12.7 a nižší)**.

   Počínaje aplikací Kaspersky Endpoint Security 12.8 pro systém Windows aplikace používá silnější šifrování hesla. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.8 nebo novější, doporučujeme zaškrtnutí tohoto políčka a použít silnější šifrování hesla. Dřívější verze aplikace nepodporují šifrování silného hesla. Chcete-li úlohu spustit, musíte políčko zaškrtnout.

Krok 3. Výběr účtu pro spuštění úlohy

Vyberte možnost **Default account**. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

Krok 4. Konfigurace plánu spuštění úlohy

V části **Scheduled start** vyberte možnost **Manually**.

Krok 5. Definování názvu úlohy

Zadejte název úlohy, například *Heslo pro připojení k hlavnímu serveru*.

Krok 6. Dokončení vytvoření úlohy

Ukončete průvodce. Zaškrtněte políčko **Run the task after the wizard finishes** nebo spusťte úlohu ručně. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

[Jak nastavit heslo pro ochranu připojení k serveru ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.
3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Administration Server connection protection**.

   c. Do pole **Task name** zadejte krátký popis, například *Heslo pro připojení k hlavnímu serveru*.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.
4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.
5. Vyberte výchozí uživatelský účet. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Ukončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na úlohu **Administration Server connection protection** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.

9. V části **Administration Server connection protection** vyberte možnost **Protect with a password**.

10. V rozevíracím seznamu **Connection to the Administration Server** vyberte možnost **New password**.

11. V poli **Password** nastavte heslo pro připojení k serveru pro správu a potvrďte je.

    Pokud heslo zapomenete, můžete si je změnit pomocí úlohy.

12. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.7 nebo dřívější verzi aplikace, zaškrtněte políčko **Enable password encryption compatibility for previous application versions (12.7 and lower)**.

    Počínaje aplikací Kaspersky Endpoint Security 12.8 pro systém Windows aplikace používá silnější šifrování hesla. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.8 nebo novější, doporučujeme zaškrtnutí tohoto políčka a použít silnější šifrování hesla. Dřívější verze aplikace nepodporují šifrování silného hesla. Chcete-li úlohu spustit, musíte políčko zaškrtnout.

13. Uložte změny.

14. Zaškrtněte políčko vedle úlohy.

15. Klikněte na tlačítko **Start**.

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

Opětovné připojení počítače k jinému serveru pro správu

Opětovné připojení počítače k jinému serveru pro správu zahrnuje následující kroky:

1. V konzole aktuálního serveru `[KSC1]` spusťte pro součást Network Agent úlohu *Change Administration Server*.

   Po provedení úlohy se počítač opětovně připojí k serveru `[KSC2]`.

   Počítač se bude zobrazovat v serverové konzole `[KSC1]` se stavem *Critical*. Konfigurace aplikace pomocí zásad nebo vzdálené spouštění úloh v počítači není možné.

2. V konzole nového serveru `[KSC2]` vytvořte novou úlohu *Ochrana připojení k serveru pro správu* pro aplikaci Kaspersky Endpoint Security. Ve vlastnostech úlohy zadejte heslo předchozího serveru a nastavte heslo pro nový server.

   Jak nastavit nové heslo pro opětovné připojení k novému serveru v konzole pro správu (MMC)

   1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

      Otevře se seznam úloh.

   2. Klikněte na tlačítko **New task**.

   Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

   #### Krok 1. Volba typu úlohy

   Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Ochrana připojení k serveru pro správu**.

   #### Krok 2. Ochrana připojení k serveru pro správu

   Nastavte heslo pro ochranu připojení k novému serveru pro správu:

   1. V části **Ochrana připojení k serveru pro správu** vyberte možnost **Chránit heslem**.

   2. V rozevíracím seznamu **Server pro správu** vyberte možnost **Znovu připojit z jiného serveru**.

   3. Do pole **Aktuální heslo** zadejte heslo nastavené pro připojení k dříve používanému důvěryhodnému serveru.

   4. V poli **Nové heslo** nastavte heslo pro připojení k novému serveru pro správu a potvrďte je.

      Pokud heslo zapomenete, můžete si je změnit pomocí úlohy.

5. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.7 nebo dřívější verzi aplikace, zaškrtněte políčko **Povolit kompatibilitu šifrování hesel pro předchozí verze aplikace (12.7 a nižší)**.

   Počínaje aplikací Kaspersky Endpoint Security 12.8 pro systém Windows aplikace používá silnější šifrování hesla. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.8 nebo novější, doporučujeme zaškrtnutí tohoto políčka a použít silnější šifrování hesla. Dřívější verze aplikace nepodporují šifrování silného hesla. Chcete-li úlohu spustit, musíte políčko zaškrtnout.

Krok 3. Výběr účtu pro spuštění úlohy

Vyberte možnost **Default account**. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

Krok 4. Konfigurace plánu spuštění úlohy

V části **Scheduled start** vyberte možnost **Manually**.

Krok 5. Definování názvu úlohy

Zadejte název úlohy, například *Heslo pro připojení k hlavnímu serveru*.

Krok 6. Dokončení vytvoření úlohy

Ukončete průvodce. Zaškrtněte políčko **Run the task after the wizard finishes** nebo spusťte úlohu ručně. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak nastavit nové heslo pro opětovné připojení k novému serveru ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Administration Server connection protection**.

   c. Do pole **Task name** zadejte krátký popis, například *Heslo pro připojení k hlavnímu serveru*.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.

5. Vyberte výchozí uživatelský účet. Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Ukončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na úlohu **Administration Server connection protection** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.

9. V části **Administration Server connection protection** vyberte možnost **Protect with a password**.

10. V rozevíracím seznamu **Connection to the Administration Server** vyberte možnost **Reconnect from another server**.

11. Do pole **Current password** zadejte heslo nastavené pro připojení k dříve používanému důvěryhodnému serveru.

12. V poli **New password** nastavte heslo pro připojení k novému serveru pro správu a potvrďte je.

    Pokud heslo zapomenete, můžete si je změnit pomocí úlohy.

13. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.7 nebo dřívější verzi aplikace, zaškrtněte políčko **Povolit kompatibilitu šifrování hesel pro předchozí verze aplikace (12.7 a nižší)**.

Počínaje aplikací Kaspersky Endpoint Security 12.8 pro systém Windows aplikace používá silnější šifrování hesla. Pokud máte nasazenou aplikaci Kaspersky Endpoint Security 12.8 nebo novější, doporučujeme zaškrtnutí tohoto políčka a použít silnější šifrování hesla. Dřívější verze aplikace nepodporují šifrování silného hesla. Chcete-li úlohu spustit, musíte políčko zaškrtnout.

14. Uložte změny.
15. Zaškrtněte políčko vedle úlohy.
16. Klikněte na tlačítko **Start**.

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

Po dokončení úlohy se ujistěte, že v konzole nového serveru `[KSC2]` má počítač stav *OK* . Otestujte, zda můžete vzdáleně spouštět úlohy a konfigurovat aplikaci pomocí zásad.

Resetování hesla pro připojení k serveru pro správu

Pokud jste zapomněli heslo pro připojení k serveru pro správu nebo bylo heslo vyzrazeno, můžete heslo obnovit ve vlastnostech úlohy. Můžete také resetovat heslo a nastavit nové heslo pro skupinu počítačů s různými stavy ochrany připojení k serveru pro správu. To znamená, že pokud je v některých počítačích ochrana povolena a v některých zakázána, úloha nastaví heslo pro všechny počítače.

Heslo pro připojení k serveru pro správu lze resetovat pouze v konzole důvěryhodného serveru, ke kterému je počítač připojen.

Jak resetovat heslo pro ochranu připojení k serveru pro správu pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Vyberte úlohu **Ochrana připojení k serveru pro správu** a dvojitým kliknutím otevřete vlastnosti této úlohy.
4. V okně vlastností úlohy vyberte část **Nastavení**.
5. V části **Ochrana připojení k serveru pro správu** vyberte možnost **Chránit a změnit heslo**.
6. V poli **Heslo pro připojení k serveru pro správu** nastavte nové heslo pro připojení k aktuálnímu důvěryhodnému serveru pro správu a potvrďte je.
7. Uložte změny.
8. Spusťte úlohu.

Jak resetovat heslo pro ochranu připojení k serveru pro správu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Administration Server connection protection** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Application settings**.
4. V části **Administration Server connection protection** vyberte možnost **Protect and change password**.
5. V poli **Password** nastavte nové heslo pro připojení k aktuálnímu důvěryhodnému serveru pro správu a potvrďte je.
6. Uložte změny.
7. Zaškrtněte políčko vedle úlohy.
8. Klikněte na tlačítko **Start**.

Po dokončení úlohy se tak resetuje heslo pro připojení k serveru pro správu.

Zakázání ochrany připojení k serveru pro správu

Ochranu připojení k serveru pro správu můžete vzdáleně resetovat pouze v konzole důvěryhodného serveru, ke kterému je počítač připojen. Ochranu můžete zakázat rovněž místně pomocí příkazového řádku.

Jak zakázat ochranu připojení k serveru v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Tasks**.
3. Vyberte úlohu **Ochrana připojení k serveru pro správu** a dvojitým kliknutím otevřete vlastnosti této úlohy.
4. V okně vlastností úlohy vyberte část **Nastavení**.
5. V části **Ochrana připojení k serveru pro správu** vyberte možnost **Nechránit**.
6. Uložte změny.
7. Spusťte úlohu.

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

Jak zaázat ochranu připojení k serveru ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Administration Server connection protection** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Application settings**.
4. V části **Administration Server connection protection** vyberte možnost **Do not protect**.
5. Uložte změny.
6. Zaškrtněte políčko vedle úlohy.
7. Klikněte na tlačítko **Start**.

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

Jak zakázat ochranu připojení k serveru pomocí 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. Spusťte následující příkaz:

   avp.com SERVERBINDINGDISABLE [/password=<password>]

   kde `<password>` je heslo k uživatelskému účtu KL Admin nebo heslo z úlohy *Ochrana připojení k serveru pro správu*. Pokud není tento parametr zadán, aplikace Kaspersky Endpoint Security vás na dalším řádku vyzve k zadání hesla.

   > Chcete-li provést tento příkaz, musí být povolena ochrana heslem.

```
Příklad
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

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.

Pokud je aplikace Kaspersky Endpoint Security nainstalována do počítače s architekturou ARM, je k dispozici pouze nástroj BitLocker Drive Encryption. Aplikace nepodporuje jiné součásti pro šifrování dat.

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 bude používat 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 Single Sign-On (SSO), 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. 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.
- Pokud je aplikace Kaspersky Endpoint Security nainstalována na počítači s architekturou ARM, je k dispozici pouze úplné šifrování disku pomocí technologie BitLocker Drive Encryption, jiné součásti šifrování nejsou podporovány.

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 ExpressCache.

- 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 ThinkCentre 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 není podporována na počítačích s architekturou ARM.

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

Spuštění nástroje 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.

Před zahájením šifrování disku musíte zkontrolovat nastavení 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. 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 (viz pokyny níže). Můžete také použít technologii SSO (Single Sign-On).

Aplikace Kaspersky Endpoint Security umožňuje automaticky vytvořit ověřovacího agenta pro tyto skupiny uživatelů:

- **Všechny účty v počítači**. Všechny účty v počítači, které byly kdykoli aktivní.
- **Všechny účty domén v počítači**. Všechny účty v počítači, které patří do nějaké domény a které byly kdykoli aktivní.
- **Všechny místní účty v počítači**. Všechny místní účty v počítači, které byly kdykoli aktivní.
- **Účet služby s jednorázovým heslem**. Účet služby je nezbytný pro získání přístupu k počítači, například když uživatel zapomene heslo. Účet služby můžete také použít jako rezervní účet. Musíte zadat název účtu (ve výchozím nastavení `ServiceAccount`). Kaspersky Endpoint Security vytvoří heslo automaticky. Heslo najdete v konzole aplikace Kaspersky Security Center.
- **Místní správce**. Kaspersky Endpoint Security vytvoří uživatelský účet ověřovacího agenta pro místního správce počítače.
- **Správce počítače**. Kaspersky Endpoint Security vytvoří uživatelský účet ověřovacího agenta pro správce počítače. Který účet má roli správce počítače, můžete zjistit ve vlastnostech počítače ve službě Active Directory. Ve výchozím nastavení není role správce počítače definována, to znamená, že neodpovídá žádnému účtu.
- **Aktivní účet**. Kaspersky Endpoint Security automaticky vytvoří účet ověřovacího agenta pro účet, který je aktivní v době šifrování disku.

Úloha *Správa účtů ověřovacího agenta* je navržena pro konfiguraci nastavení ověření uživatele. Pomocí této úlohy můžete přidat nové účty, upravit nastavení aktuálních účtů nebo v případě potřeby účty odebrat. Můžete použít místní úkoly pro jednotlivé počítače i skupinové úkoly pro počítače ze samostatných skupin správy nebo z výběru počítačů.

Jak spustit Kaspersky Disk Encryption pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.

4. 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.

5. V rozevíracím seznamu **Režim šifrování** vyberte možnost **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.

6. Nakonfigurujte rozšířené možnosti technologie Kaspersky Disk Encryption (viz tabulka níže).

7. Uložte změny.

Jak spustit Kaspersky Disk Encryption prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Data Encryption** → **Full Disk Encryption**.

5. Vyberte technologii **Kaspersky Disk Encryption**.

   Technologii Kaspersky Disk Encryption nelze použít, jestliže počítač obsahuje pevné disky, které byly šifrované nástrojem BitLocker.

6. V bloku **Action on devices** vyberte položku **Encrypt all hard drives**.

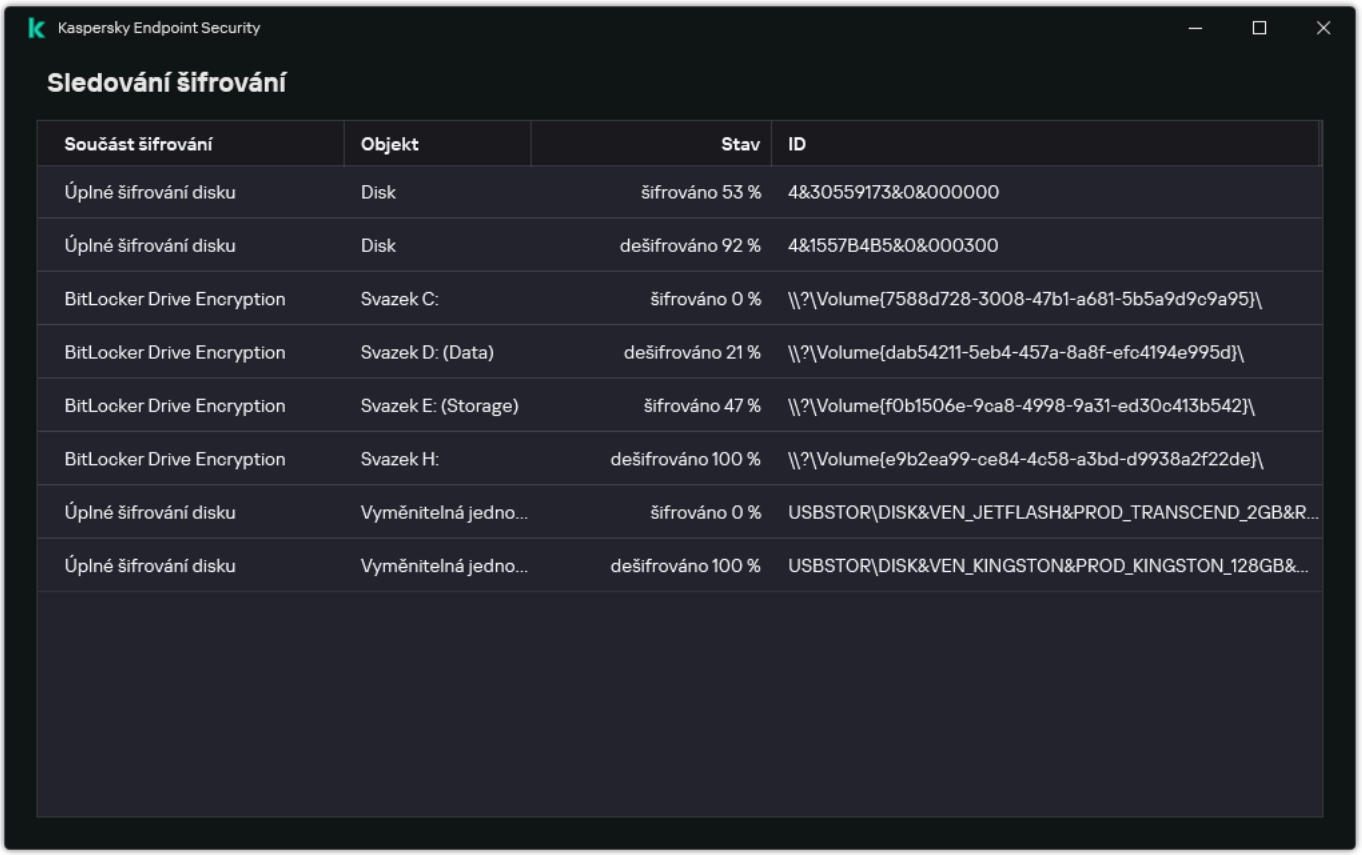
   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém bylo provedeno šifrování.

   Pokud potřebujete vyloučit některé pevné disky ze šifrování, vytvořte pro tyto pevné disky seznam.

7. Nakonfigurujte rozšířené možnosti technologie Kaspersky Disk Encryption (viz tabulka níže).

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.



Sledování šifrování

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.

Nastavení součásti Kaspersky Disk Encryption

Parametr	Popis
Automaticky vytvářet účty ověřovacího agenta pro uživatelé při šifrování	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*.
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 (zkracuje dobu šifrování)	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 toto nastavení nemění, dokud nejsou dešifrovány pevné disky. 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.

Ve výchozím nastavení není toto políčko zaškrtnuté.

Použít funkci Legacy USB Support (nedoporučuje se)

Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat 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.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.
4. 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.
5. Postup přidání pevných disků na seznam pevných disků vyloučených ze šifrování:
   a. Klikněte na tlačítko **Přidat**.
   b. V okně, které se otevře, zadejte hodnoty pro **Název zařízení**, **Počítač**, **Typ disku**, **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**.
6. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.
4. 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**.
5. 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 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. Uložte soubor.

Aplikace Kaspersky Endpoint Security exportuje celý seznam výjimek do souboru XML.

6. 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. Otevřete soubor.

Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru XML přidá nové položky.

7. Uložte změny.

[Jak exportovat a importovat seznam výjimek z šifrování pevného disku ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Full Disk Encryption**.
   Vyberte technologii **Kaspersky Disk Encryption**.
5. Klikněte na odkaz **Exclusions**.
   Otevře se seznam výjimek.
6. Postup exportu seznamu pravidel:

   a. Vyberte výjimky, které chcete exportovat.

   b. Klikněte na tlačítko → **Export**.
   Aplikace Kaspersky Endpoint Security exportuje seznam výjimek do souboru JSON ve výchozí složce pro stahování.
7. Postup importu seznamu výjimek:

   a. Klikněte na tlačítko → **Import**.
   V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat seznam výjimek.

   b. Otevřete soubor.
   Pokud počítač již seznam výjimek obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k němu do souboru JSON přidá nové položky.
8. Uložte změny.

Povolení technologie SSO (Single Sign-On)

Technologie Single Sign-On (SSO) umožňuje automatické přihlašování k operačnímu systému pomocí přihlašovacích údajů ověřovacího agenta. To znamená, že uživatel musí zadat heslo pouze jednou (heslo účtu ověřovacího agenta) při přihlašování do systému Windows. Technologie jednotného přihlašování také umožňuje automaticky aktualizovat heslo účtu ověřovacího agenta při změně hesla účtu systému Windows.

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.

Povolení technologie SSO (Single Sign-On)

Jak povolit použití technologie SSO konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Běžné nastavení šifrování**.
4. V bloku **Nastavení hesla** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, zaškrtněte na kartě **Ověřovací agent** políčko **Použít technologii SSO (Single Sign-On)**.
6. Pokud používáte externího poskytovatele přihlašovacích údajů, zaškrtněte políčko **Používat u externích poskytovatelů přihlašovacích údajů wrap**.
7. 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 **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Full Disk Encryption**.
5. Vyberte technologii **Kaspersky Disk Encryption**.
6. V bloku **Password settings** zaškrtněte políčko **Use Single Sign-On (SSO) technology**.
7. Pokud používáte externího poskytovatele přihlašovacích údajů, zaškrtněte políčko **Wrap third-party credential providers**.
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.

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. Tyto akce je nutno provést pouze jednou za účelem synchronizace hesel. Poté Kaspersky Endpoint Security nahradí heslo účtu ověřovacího agenta heslem účtu systému Windows. Při změně hesla účtu systému Windows aplikace automaticky aktualizuje heslo účtu ověřovacího agenta.

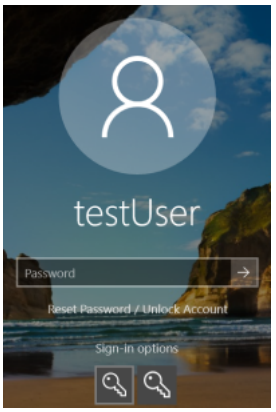
Externí poskytovatelé přihlašovacích údajů

Kaspersky Endpoint Security podporuje externího poskytovatele přihlašovacích údajů ADSelfService Plus.

Při práci s externími poskytovateli přihlašovacích údajů zachytí ověřovací agent heslo ještě před načtením operačního systému. To znamená, že uživatel musí zadat heslo pouze jednou při přihlašování do systému Windows. Po přihlášení do systému Windows může uživatel využít možnosti externího poskytovatele přihlašovacích údajů například pro ověřování v podnikových službách. Externí poskytovatelé přihlašovacích údajů také umožňují uživatelům nezávisle resetovat vlastní heslo. V tomto případě aplikace Kaspersky Endpoint Security aktualizuje heslo pro ověřovacího agenta automaticky.

Pokud používáte externího poskytovatele přihlašovacích údajů, který není podporován aplikací, můžete se setkat s určitými omezeními při provozu technologie jednotného přihlašování. Při přihlašování do systému Windows má uživatel k dispozici dva profily: systémového poskytovatele přihlašovacích údajů a externího poskytovatele přihlašovacích údajů. Ikony těchto profilů budou shodné (viz obrázek níže). Uživatel bude mít k dispozici následující možnosti, jak pokračovat:

- Pokud uživatel vybere *externího poskytovatele přihlašovacích údajů*, nebude ověřovací agent schopen synchronizovat heslo s účtem systému Windows. Pokud tedy uživatel změnil heslo účtu systému Windows, nemůže aplikace Kaspersky Endpoint Security aktualizovat heslo účtu ověřovacího agenta. Uživatel pak musí provést ověření dvakrát: v rozhraní ověřovacího agenta a před načtením operačního systému. V tomto případě může uživatel využít možnosti externího poskytovatele přihlašovacích údajů například pro ověřování v podnikových službách.
- Pokud uživatel vybere *systémového poskytovatele přihlašovacích údajů*, ověřovací agent synchronizuje heslo s účtem systému Windows. V tomto případě uživatel nemůže využít možnosti externího poskytovatele například pro ověřování v podnikových službách.



Systémový profil ověřování a externí profil ověřování pro přihlašování do 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **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 **Run the task after the wizard finishes**. 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 konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows (14.0)**.
2. V rozevíracím seznamu **Task type** vyberte možnost **Manage Authentication Agent accounts**.
3. Do pole **Task name** zadejte krátký popis, například *Účty správce*.
4. V bloku **Devices to which the task will be assigned** 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

Ukončete 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. Ve vlastnostech úlohy vyberte část **Nastavení**.
3. Klikněte na možnosti **Přidat** → **Příkaz přidání účtu**.
4. V okně, které se otevře, zadejte do pole **Účet 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 dostupný, když přidáváte příkaz k vytvoření účtu ověřovacího agenta do vlastností místní úlohy *Správa účtů ověřovacího agenta*.

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. V bloku **Přístup k ověření v ověřovacím agentovi** nakonfigurujte přístup k ověření v ověřovacím agentovi pro uživatele, který používá účet zadaný v příkazu.
12. Uložte změny.

Jak přidat účet ověřovacího agenta prostřednictvím webové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Manage Authentication Agent accounts** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Application settings**.
4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Add**.

   Spustí se průvodce správou účtů ověřovacího agenta.
5. Vyberte typ příkazu **Add**.
6. Vyberte uživatelský účet. Účet můžete vybrat ze seznamu doménových účtů nebo ručně zadat název účtu. Přejděte k dalšímu kroku.

   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.
   - **Create a new Authentication Agent account to replace the existing account**. 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.
   - **User name**. Výchozí uživatelské jméno účtu ověřovacího agenta se shoduje názvu domény uživatele.
   - **Allow password-based authentication**. 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.
   - **Allow certificate-based authentication**. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu. Uživatel tak bude muset zadat heslo pro čipovou kartu nebo token.
   - **Account access to encrypted data**. Zde můžete nakonfigurovat přístup uživatele k šifrované jednotce. Můžete například namísto odstranění účtu ověřovacího agenta dočasně zakázat ověřování uživatelů.
   - **Comment**. V případě potřeby zadejte popis účtu.
8. Uložte změny.
9. 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 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. Ve vlastnostech úlohy vyberte část **Nastavení**.
3. Klikněte na možnosti **Přidat** → **Příkaz úprav účtu**.
4. V okně, které se otevře, zadejte do pole **Účet 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 konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.
2. Klikněte na úlohu **Manage Authentication Agent accounts** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.
3. Vyberte kartu **Application settings**.
4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Add**.

   Spustí se průvodce správou účtů ověřovacího agenta.
5. Vyberte typ příkazu **Change**.

6. Vyberte uživatelský účet. Účet můžete vybrat ze seznamu doménových účtů nebo ručně zadat název účtu. Přejděte k dalšímu kroku.

   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.

   - **Create a new Authentication Agent account to replace the existing account**. 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.
   - **User name**. Výchozí uživatelské jméno účtu ověřovacího agenta se shoduje názvu domény uživatele.
   - **Allow password-based authentication**. 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.
   - **Allow certificate-based authentication**. Vyberte soubor certifikátu pro ověření pomocí čipové karty nebo tokenu. Uživatel tak bude muset zadat heslo pro čipovou kartu nebo token.
   - **Account access to encrypted data**. Zde můžete nakonfigurovat přístup uživatele k šifrované jednotce. Můžete například namísto odstranění účtu ověřovacího agenta dočasně zakázat ověřování uživatelů.
   - **Comment**. V případě potřeby zadejte popis účtu.

9. Uložte změny.

10. Zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**.

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. Ve vlastnostech úlohy vyberte část **Nastavení**.

3. Klikněte na možnosti **Přidat** → **Příkaz odstranění účtu**.

4. V okně, které se otevře, do pole **Účet 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 konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **Manage Authentication Agent accounts** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Application settings**.

4. V seznamu účtů ověřovacího agenta klikněte na tlačítko **Add**.

   Spustí se průvodce správou účtů ověřovacího agenta.

5. Vyberte typ příkazu **Delete**.

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 **Start**.

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 stromu konzoly vyberte možnost **Devices**.

3. Dvojitým kliknutím otevřete okno vlastností počítače.

4. V okně vlastností počítače vyberte část **Tasks**.

5. V seznamu úloh vyberte úlohu **Správa účtů ověřovacího agenta** a dvojitým kliknutím otevřete její vlastnosti.

6. Ve vlastnostech 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 konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.

2. Klikněte na název počítače, na kterém chcete zobrazit seznam účtů ověřovacího agenta.

3. Ve vlastnostech počítače vyberte kartu **Tasks**.

4. V rozevíracím seznamu vyberte možnost **Manage Authentication Agent accounts**.

5. Ve vlastnostech úlohy vyberte část **Application settings**.

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
- 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

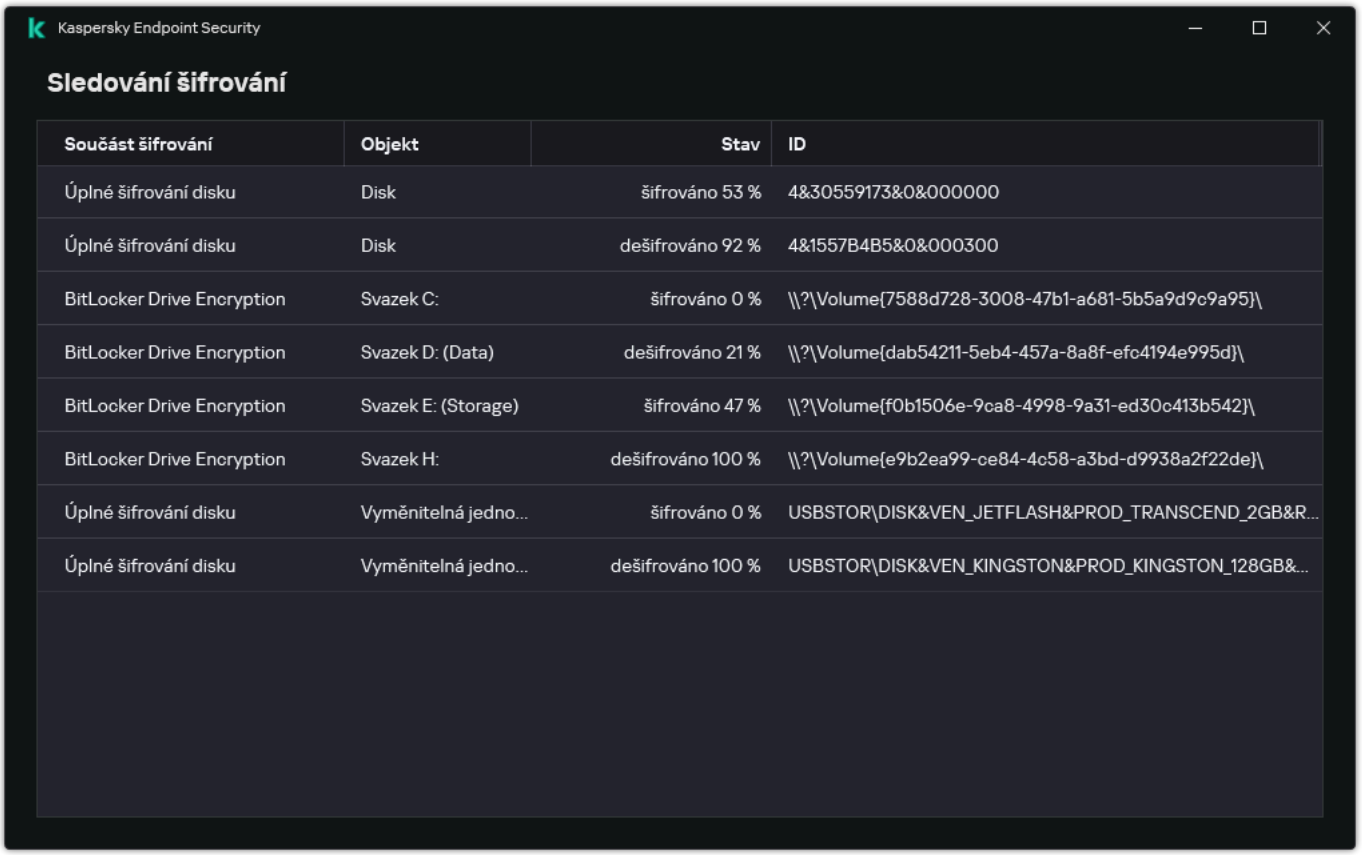
Pevné disky můžete dešifrovat, i když není k dispozici žádná aktuální licence povolující šifrování dat.

Postup dešifrování pevných disků:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.
4. V rozevíracím seznamu **Technologie šifrování** vyberte technologii, pomocí které byly pevné disky šifrovány.
5. 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.
6. 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.



Sledování šifrování

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).

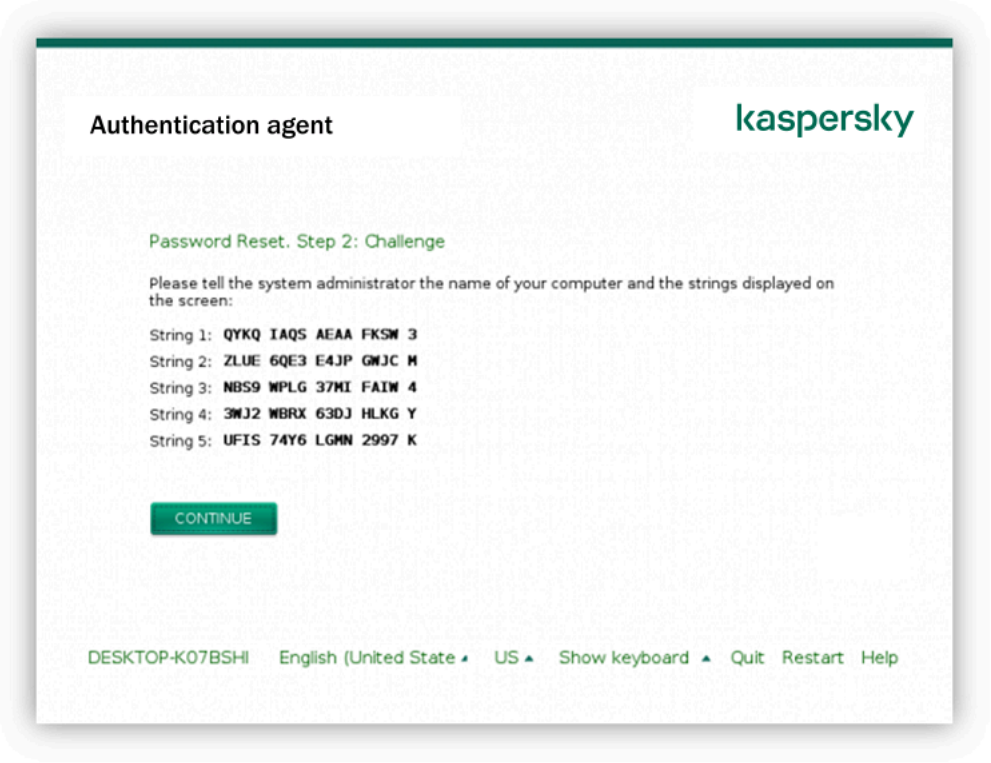
Obnovení přístupu k jednotce chráněné technologií Kaspersky Disk Encryption

Pokud uživatel zapomněl heslo pro přístup k pevnému disku chráněnému technologií Kaspersky Disk Encryption, musí zahájit proces obnovení (žádost–odpověď). Můžete také pomocí účtu služby získat přístup k pevnému disku, pokud je tato funkce povolena v nastavení šifrování disku.

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

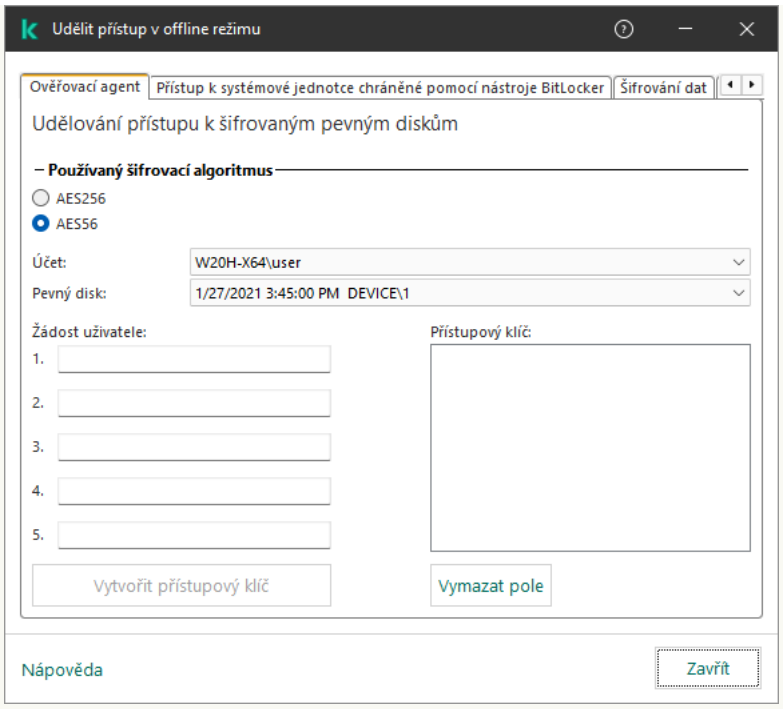
Chce-li uživatel zahájit proces obnovení, musí v rozhraní ověřovacího agenta kliknout na tlačítko **Forgot your password**.

[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 stromu konzoly vyberte možnost **Devices**.
3. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
4. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
5. Tím otevřete okno; v tomto okně vyberte kartu **Ověřovací agent**.
6. V bloku **Používaný šifrovací algoritmus** vyberte šifrovací algoritmus: **AES56** nebo **AES256**.

   Algoritmus šifrování dat závisí na šifrovací knihovně AES, která je součástí distribučního balíčku: *Strong encryption (AES256)* nebo *Lite encryption (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.
7. V rozevíracím seznamu **Účet** vyberte název účtu ověřovacího agenta vytvořeného pro uživatele, který požaduje obnovení přístupu k disku.
8. V rozevíracím seznamu **Pevný disk** vyberte šifrovaný pevný disk, u kterého potřebujete obnovit přístup.
9. V bloku **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.



Udělit přístup v offline režimu

Jak získat bloky odpovědi pro systémový pevný disk chráněný technologií Kaspersky Disk Encryption ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.
3. Klikněte na tlačítko **Grant access to the device in offline mode**.
4. V okně, které se otevře, vyberte část **Authentication Agent**.
5. V rozevíracím seznamu **Account** 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 stromu konzoly vyberte možnost **Devices**.

3. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.

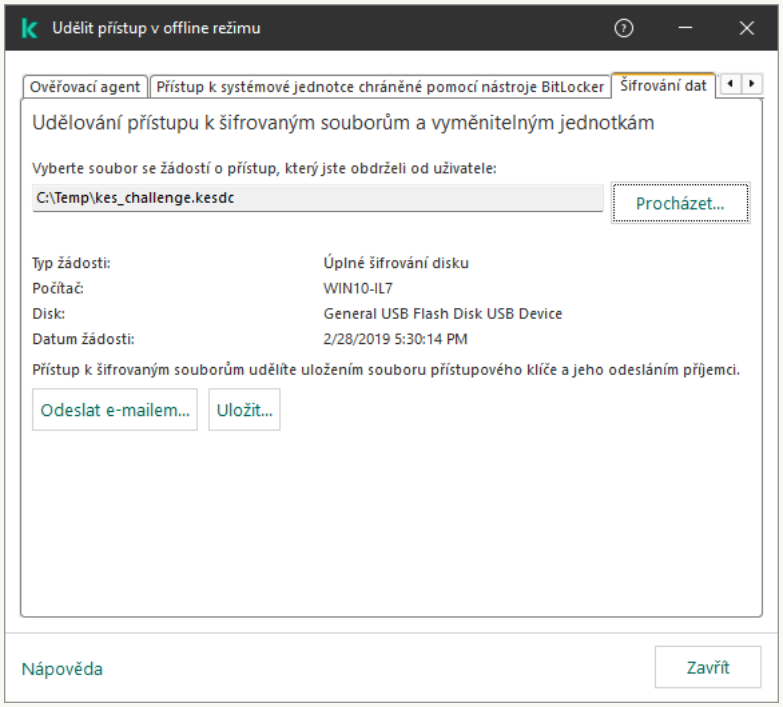
4. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.

5. Tím otevřete okno; v tomto okně vyberte kartu **Šifrování dat**.

6. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.

7. 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.



Udělit přístup v offline režimu

[Jak získat soubor klíče šifrovaného přístupu k nesystémovému pevnému disku ve webové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.

2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.

3. Klikněte na tlačítko **Grant access to the device in offline mode**.

4. Vyberte možnost **Data Encryption**.

5. Klikněte na tlačítko **Select file** 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 **Save key** 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.

Přihlášení pomocí účtu služby ověřovacího agenta

Aplikace Kaspersky Endpoint Security umožňuje při šifrování jednotky přidat účet služby ověřovacího agenta. Účet služby je nezbytný pro získání přístupu k počítači, například když uživatel zapomene heslo. Účet služby můžete také použít jako rezervní účet. Chcete-li přidat účet, vyberte účet služby nastavení šifrování disku a zadejte název uživatelského účtu (ve výchozím nastavení `ServiceAccount`). K ověření pomocí agenta budete potřebovat jednorázové heslo.

[Jak zjistit jednorázové heslo v konzole pro správu (MMC)]

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Devices**.
3. Dvojitým kliknutím otevřete okno vlastností počítače.
4. V okně vlastností počítače vyberte část **Tasks**.
5. V seznamu úloh vyberte úlohu **Správa účtů ověřovacího agenta** a dvojitým kliknutím otevřete její vlastnosti.
6. V okně vlastností úlohy vyberte část **Nastavení**.
7. V seznamu účtů vyberte účet služby ověřovacího agenta (např. `WIN10-USER\ServiceAccount`).
8. V rozevíracím seznamu **Akce** vyberte možnost **Zobrazit účet**.
9. Ve vlastnostech účtu zaškrtněte políčko **Zobrazit původní heslo**.
10. Zkopírujte si jednorázové heslo pro přihlášení pomocí účtu služby.

Jak zjistit jednorázové heslo ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Klikněte na název počítače, na kterém chcete zobrazit seznam účtů ověřovacího agenta.
   Otevřou se vlastnosti počítače.
3. Ve vlastnostech počítače vyberte kartu **Tasks**.
4. V rozevíracím seznamu vyberte možnost **Manage Authentication Agent accounts**.
5. Ve vlastnostech úlohy vyberte část **Application settings**.
6. V seznamu účtů vyberte účet služby ověřovacího agenta (např. `WIN10-USER\ServiceAccount`).
7. Ve vlastnostech účtu zaškrtněte políčko **Show password**.
8. Zkopírujte si jednorázové heslo pro přihlášení pomocí účtu služby.

Kaspersky Endpoint Security automaticky aktualizuje heslo pokaždé, když se uživatel ověří pomocí účtu služby. Po ověření pomocí agenta musíte zadat heslo účtu systému Windows. Při přihlašování pomocí účtu služby nemůžete používat technologii SSO.

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.

Funkce aktualizace operačního systému:

- **Aktualizace operačního systému prostřednictvím WSUS**. Operační systém můžete aktualizovat běžným způsobem.
- **Aktualizace operačního systému z ISO**. Chcete-li aktualizovat operační systém, musíte určit složku s ovladači Kaspersky Disk Encryption. Aplikace automaticky zkopíruje ovladače do samostatné složky. Postupujte následovně:

  1. Nasaďte bitovou kopii ISO.
  2. Spusťte instalaci aktualizace systému pomocí následujícího klíče:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.0\reflect_drivers
     ```

Automatická aktualizace operačního systému je k dispozici, pouze pokud počítač používá systém Windows 10 1607 (RS1) nebo novější. Chcete-li upgradovat dřívější verze operačního systému, doporučujeme nejprve dešifrovat disk, provést upgrade operačního systému a poté disk zašifrovat.

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 14.0.

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 upgradu funkce Úplné šifrování disku bylo dokončeno s chybou.

Chcete-li odstranit chyby, ke kterým došlo během procesu aktualizace funkce Úplné šifrování disku,

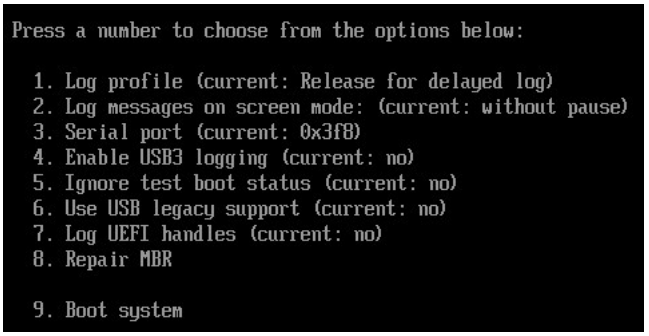
obnovte přístup k šifrovaným zařízením pomocí nástroje pro obnovení.

Trasování ověřovacího agenta

Aplikace do souboru trasování protokoluje informace o provozu a uživatelském využití ověřovacího agenta.

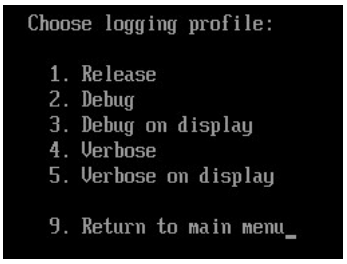
Postup povolení trasování ověřovacího agenta:

1. Povolte trasování aplikace Kaspersky Endpoint Security.
2. Restartujte počítač.
3. Ihned po zapnutí počítače se šifrovanými pevnými disky vyvolejte stisknutím klávesy **F3** okno ke konfiguraci nastavení ověřovacího agenta.
4. Po spuštění zavaděče FDE vyberte správce spouštění **KES (FDE <version>)**.
5. V nabídce správce spouštění přejděte na nastavení **Log profile**.



Nabídka správce spouštění

6. Vyberte úroveň trasování v okně nastavení profilu protokolu:



Úrovně trasování ověřovacího agenta

- **Release**. Pokud je zvolena tato možnost, aplikace do souboru trasování neprotokoluje informace o událostech ověřovacího agenta.
- **Debug**. Pokud je zvolena tato možnost, aplikace do souboru trasování protokoluje informace o provozu a uživatelském využití ověřovacího agenta.
- **Debug on display**. 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.
- **Verbose**. 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 **Debug**. Vyšší úroveň podrobnosti záznamů může zpomalit spouštění ověřovacího agenta a operačního systému.
- **Verbose on display**. 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 **Debug on display**. Vyšší úroveň podrobnosti záznamů může zpomalit spouštění ověřovacího agenta a operačního systému.

Poté, co vyberete úroveň trasování, správce spouštění znovu zobrazí nabídku.

7. V nabídce správce spouštění vyberte možnost **Boot system**.

   Zavaděč FDE spustí ověřovacího agenta.

   Reprodukujte problém.

   Data jsou zaznamenávána do souboru trasování ověřovacího agenta, pokud jsou v počítači přítomny šifrované pevné disky nebo během úplného šifrování disku.
8. Chcete-li zastavit proces trasování, vraťte se do okna Nástroje podpory a zakažte trasování.

Soubory trasování provozu KES.SRV ověřovacího agenta se tak vytvářejí ve složce `%ProgramData%\Kaspersky Lab\KES.14.0\Traces`. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Běžné nastavení šifrování**.
4. V bloku **Šablony** klikněte na tlačítko **Nápověda**.
5. V okně, které se otevře, postupujte takto:
   - Vyberte kartu **Ověření** a upravte text nápovědy zobrazující se v okně ověřovacího agenta během zadávání přihlašovacích údajů účtu.
   - Vyberte kartu **Změnit heslo** a upravte text nápovědy zobrazující se v okně ověřovacího agenta při změně hesla pro účet ověřovacího agenta.

- Vyberte kartu **Obnovit heslo** a upravte text nápovědy zobrazující se v okně ověřovacího agenta při obnovování hesla pro účet ověřovacího agenta.

6. 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.

7. 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.

Použití Nástroje pro obnovení k odstranění objektů a dat, které zůstaly po testovacím provozu Ověřovacího agenta:

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 Nástroj pro obnovení vyberte požadované zařízení.
3. Klikněte na tlačítko **Kontrolovat**.
4. Pokud se po diagnostice systémového pevného disku zobrazí zpráva s informací, že po testovacím provozu Ověřovacího agenta zůstaly objekty a data, klikněte na **Odstranit objekty a data AA**.

   Tlačítko **Odstranit objekty a data AA** je k dispozici pouze v případě, že jsou zjištěny objekty a data, které zůstaly po testovacím provozu Ověřovacího agenta.

Chcete-li odstranit informace o nekompatibilitě aplikací s ověřovacím agentem,

zadejte do příkazového řádku příkaz `avp pbatestreset`.

Správa nástroje BitLocker

BitLocker je šifrovací technologie zabudovaná do operačních systémů Windows. Aplikace Kaspersky Endpoint Security vám umožňuje řídit a spravovat technologii Bitlocker pomocí infrastruktury Kaspersky Next. BitLocker šifruje logické svazky. BitLocker nelze použít pro šifrování vyměnitelných jednotek. Podrobnosti o technologii BitLocker najdete v dokumentaci společnosti Microsoft.

Při šifrování disku BitLocker vloží zavaděč a další pomocné soubory do tohoto umístění: system partition. Tento oddíl není šifrován. Operační systém vytvoří systémový oddíl automaticky během instalace systému Windows. Pokud je disk před instalací systému Windows plně rozdělen na oddíly, operační systém nemůže vytvořit systémový oddíl. V tomto případě vás při spuštění šifrování disku BitLocker vyzve operační systém, aby znovu vytvořil oblasti na disku a vytvořil systémový oddíl. Po vytvoření systémového oddílu operační systém spustí šifrování BitLocker.

Šifrovací algoritmus algoritmu BitLocker nezávisí na verzi knihovny AES zahrnuté v distribučním balíčku (AES256 nebo AES56). Šifrování používá integrovanou knihovnu šifrování operačního systému.

Ve výchozím nastavení používá aplikace k šifrování zařízení, která nikdy nebyla šifrována, šifrovací algoritmus BitLocker s efektivní délkou klíče 256 bitů. U zařízení, které bylo před instalací aplikace zašifrováno, se může šifrovací algoritmus lišit. Podrobné informace o výběru šifrovacího algoritmu najdete na webu technické podpory společnosti Microsoft. Počínaje verzí 12.9 odesílá aplikace Kaspersky Endpoint Security originální obnovovací klíč pro zařízení, která byla dříve zašifrována aplikacemi třetích stran, do aplikace Kaspersky Security Center.

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 systémového pevného disku musí uživatel před spuštěním operačního systému projít ověřením nástrojem BitLocker. Po ověření umožňuje BitLocker uživateli přihlášení. BitLocker nepodporuje technologii jednotného přihlašování (SSO).

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.

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.
4. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **BitLocker Drive Encryption**.
5. V rozevíracím seznamu **Režim šifrování** vyberte možnost **Šifrovat všechny pevné disky**.

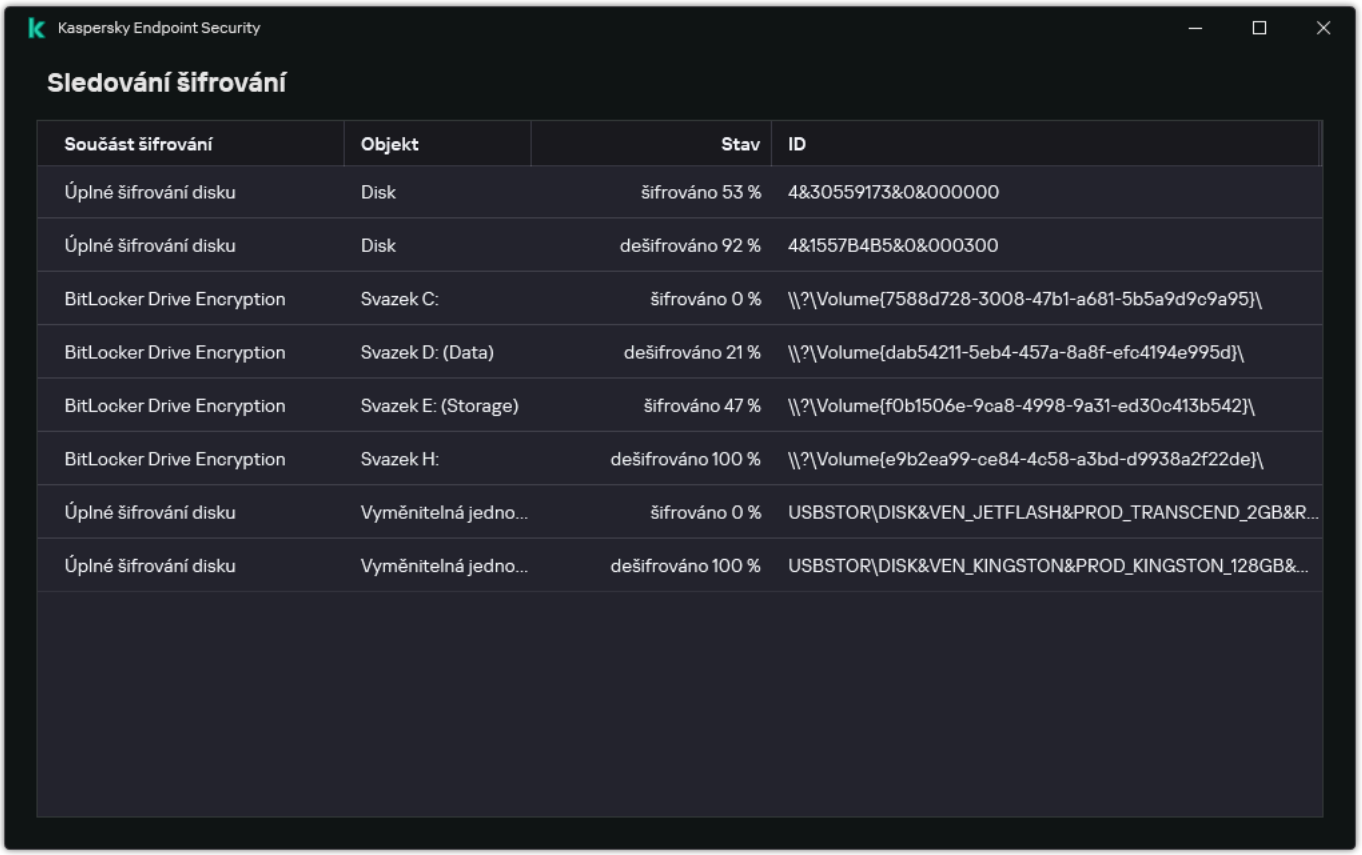
   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém bylo provedeno šifrování.
6. Nakonfigurujte rozšířené možnosti součásti BitLocker Drive Encryption (viz tabulka níže).
7. Uložte změny.

Jak spustit BitLocker Drive Encryption prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Full Disk Encryption**.
5. Vyberte technologii **BitLocker Disk Encryption**.
6. V bloku **Action on devices** vyberte položku **Encrypt all hard drives**.

   Pokud je v počítači nainstalováno několik operačních systémů, budete moci po šifrování načíst pouze systém, ve kterém bylo provedeno šifrování.
7. Nakonfigurujte rozšířené možnosti součásti BitLocker Drive Encryption (viz tabulka níže).
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.



Sledování šifrování

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	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 toto nastavení nemění, dokud nejsou dešifrovány pevné disky. 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.

Ve výchozím nastavení není toto políčko zaškrtnuté.

Způsob ověření

Pouze 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.

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.
- **TPM (Trusted Platform Module) nebo heslo, pokud TPM není k dispozici**. Pokud je tato volba vybraná, 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.

Vybranou metodu ověřování je třeba nakonfigurovat zadáním požadavků na heslo nebo PIN:

- **Minimální délka kódu PIN (znaky)**.
- **Minimální délka hesla (znaky)**.
- **Omezit dobu platnosti hesla / kódu PIN pro TPM (dny)**.
- **Povolit používání rozšířeného kódu PIN (písmena a čísla)**. *Rozšířený PIN* umožňuje kromě numerických znaků používat i další znaky: velká a malá písmena latinky, speciální znaky a mezery.

Automaticky znovu vytvořit obnovovací klíč (dny)

Automatická aktualizace hesla pro obnovení přístupu k pevnému disku chráněnému nástrojem BitLocker. Pokud je políčko zaškrtnuto, zadejte dobu platnosti hesla klíče pro obnovení. To pomáhá zabránit opakovanému použití hesla klíče pro obnovení.

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.

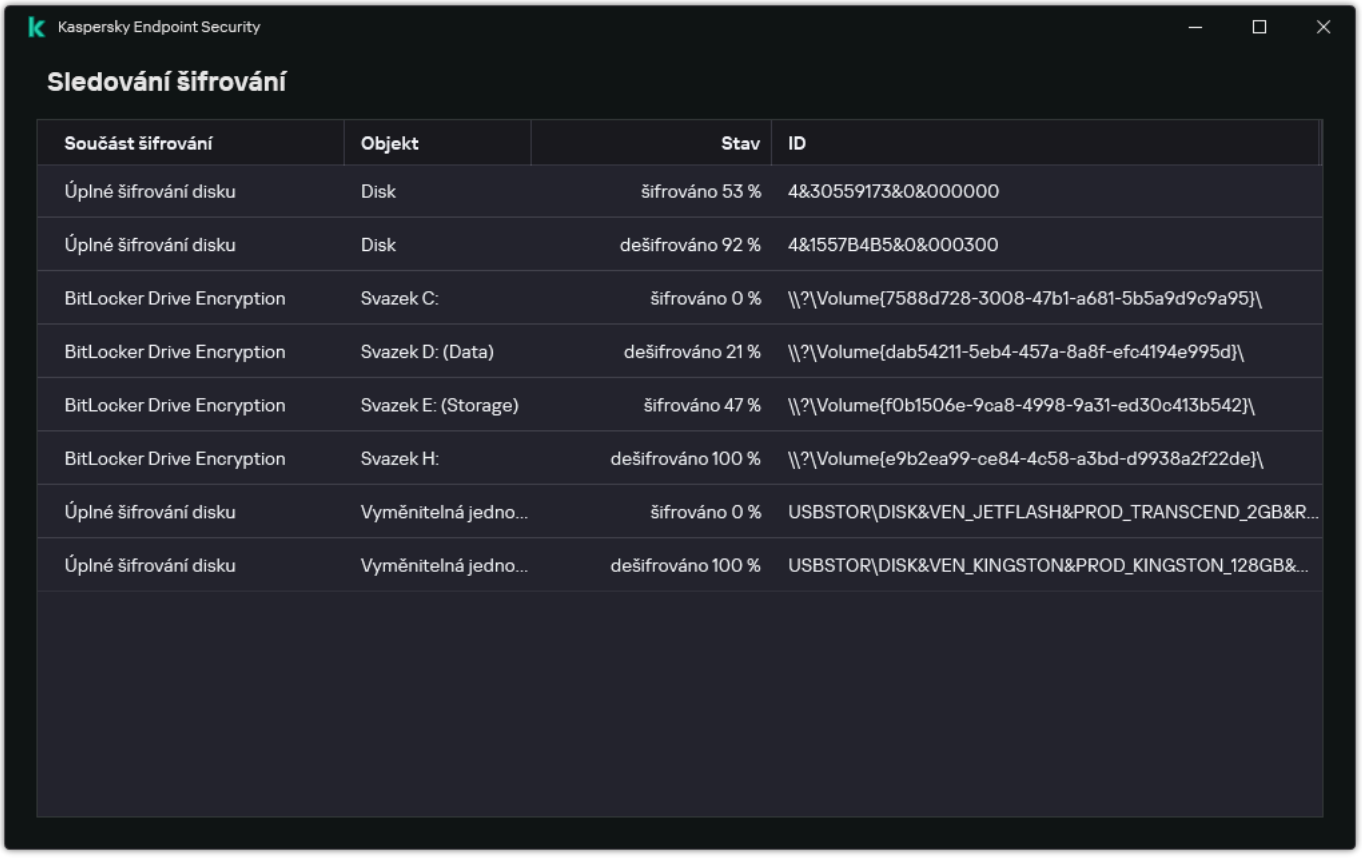
Jak dešifrovat pevný disk chráněný nástrojem BitLocker pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Úplné šifrování disku**.
4. V rozevíracím seznamu **Technologie šifrování** vyberte možnost **BitLocker Drive Encryption**.
5. V rozevíracím seznamu **Režim šifrování** vyberte možnost **Dešifrovat všechny pevné disky**.
6. Uložte změny.

Jak dešifrovat pevný disk šifrovaný pomocí nástroje BitLocker prostřednictvím webové konzoly a cloudové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Full Disk Encryption**.
5. Vyberte technologii **BitLocker Disk Encryption**.
6. V bloku **Action on devices** vyberte položku **Decrypt all hard drives**.
7. 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.



Sledování šifrování

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 (FIPS), 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:

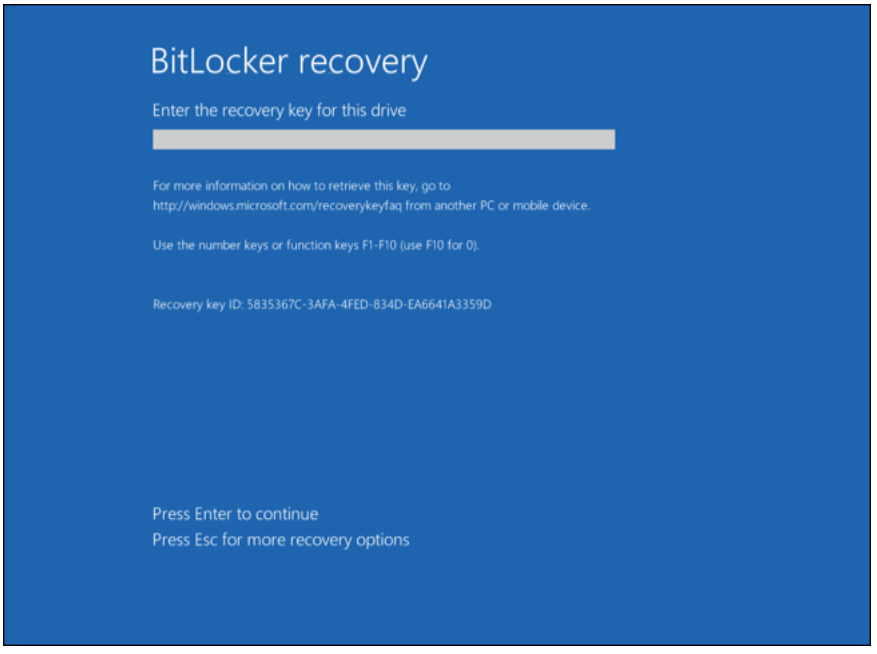
1. Uživatel sdělí správci ID obnovovacího klíče (viz obrázek níže).
2. Správce toto ID ověří ve vlastnostech počítače v aplikaci Kaspersky Security Center. ID poskytnuté uživatelem se musí shodovat s ID zobrazeným ve vlastnostech počítače.
3. Pokud se ID obnovovacího klíče shodují, správce poskytne uživateli 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.

   Pokud nechcete, aby se heslo k obnovovacímu klíči používalo opakovaně, můžete v nastavení zásad nakonfigurovat automatickou aktualizaci hesla.
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 stromu konzoly vyberte možnost **Managed devices**.
3. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.

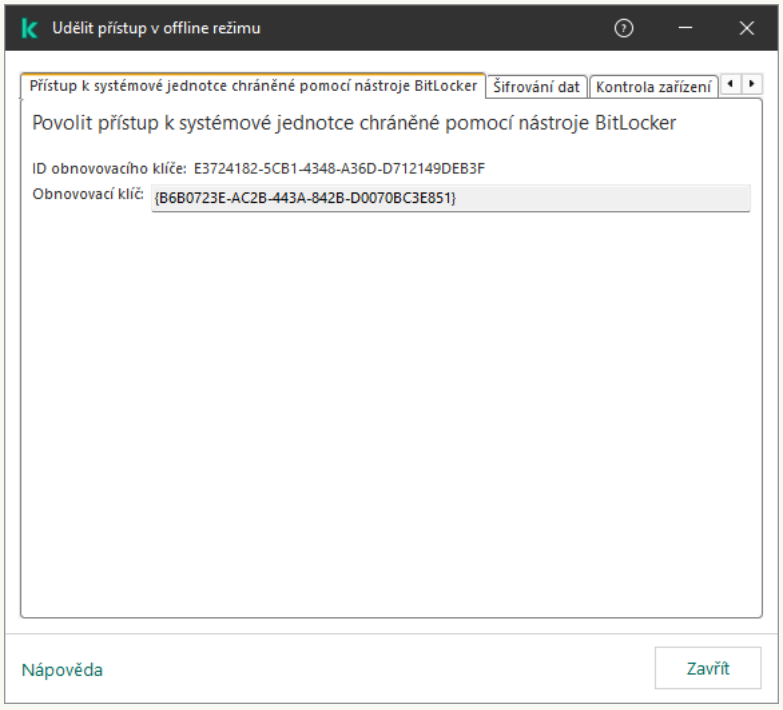
4. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.

5. Tím otevřete okno; v tomto okně vyberte kartu **Přístup k systémové jednotce chráněné pomocí nástroje BitLocker**.

6. 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.



Obnovení přístupu k disku zašifrovanému nástrojem BitLocker

[Jak zobrazit obnovovací klíč systémové jednotky zašifrované pomocí nástroje BitLocker ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.

2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.

3. Klikněte na tlačítko **Grant access to the device in offline mode**.

4. V okně, které se otevře, vyberte část **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 **Receive key**.

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

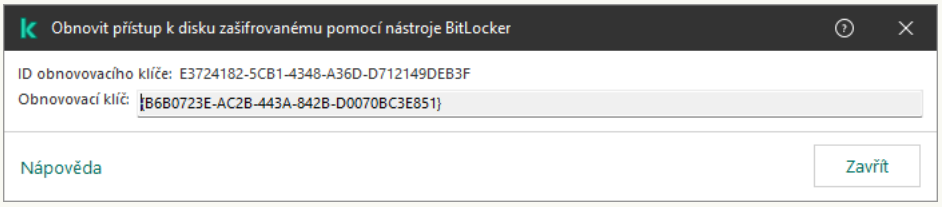
Chce-li uživatel zahájit proces obnovení, musí v okně udělujícím přístup k jednotce kliknout na odkaz **Zapomněli jste heslo**. Po získání přístupu k šifrované jednotce může uživatel povolit automatické odblokování jednotky během ověřování Windows v nastavení nástroje BitLocker.

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 konzoly pro správu vyberte možnosti **Advanced** → **Data encryption and protection** → složku **Encrypted drives**.
3. Vyberte v pracovním prostoru šifrované zařízení, pro které chcete vytvořit soubor přístupového klíče, a v kontextové nabídce zařízení klikněte na **Přístup k zařízení můžete získat v produktu Kaspersky Endpoint Security**.
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**.



Obnovení přístupu k disku zašifrovanému nástrojem BitLocker

Jak zobrazit obnovovací klíč nesystémové jednotky zašifrované pomocí nástroje BitLocker ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Operations** → **Data encryption and protection** → **Encrypted drives**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož jednotce chcete obnovit přístup.
3. Klikněte na tlačítko **Grant access to the device in offline mode**.

   Tím se spustí průvodce pro udělení přístupu k zařízení.
4. Při udělování přístupu k zařízení postupujte podle pokynů průvodce:

   a. Vyberte modul plug-in **Kaspersky Endpoint Security for 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 **Receive key**.

Díky tomu budete mít přístup k obnovovacímu klíči nebo souboru obnovovacího klíče, který bude muset být předán uživateli.

Pozastavení ochrany BitLocker kvůli aktualizaci softwaru

Při aktualizaci operačního systému, instalaci aktualizačních balíčků pro operační systém nebo aktualizaci jiného softwaru se zapnutou ochranou BitLocker existuje řada zvláštních hledisek. Instalace aktualizací může vyžadovat několikeré restartování počítače. Po každém restartu musí uživatel provést ověření nástrojem BitLocker. Abyste zajistili správnou instalaci aktualizací, můžete dočasně vypnout ověřování nástrojem BitLocker. V tomto případě disk zůstane šifrovaný a uživatel má přístup k datům po přihlášení do systému. Ke správě ověřování nástrojem BitLocker můžete použít úlohu *Správa ochrany nástrojem BitLocker*. Pomocí této úlohy můžete určit počet restartů počítače, která nevyžadují ověření BitLocker. Po instalaci aktualizací a dokončení úlohy *Správa ochrany nástrojem BitLocker* je ověřování nástrojem BitLocker automaticky povoleno. Ověření nástrojem BitLocker můžete kdykoli povolit.

Jak pozastavit ochranu nástrojem BitLocker pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0)** → **Správa ochrany nástrojem BitLocker**.

Krok 2. Správa ochrany BitLocker

Konfigurace ověřování nástrojem BitLocker. Chcete-li pozastavit ochranu BitLocker, vyberte možnost **Dočasně povolit přeskočit ověřování BitLocker** a zadejte počet restartů bez ověření nástrojem BitLocker (1- až 15krát). V případě potřeby zadejte datum a čas vypršení platnosti úlohy. V uvedenou dobu se úloha automaticky vypne a uživatel musí po restartování počítače provést ověření BitLocker.

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 například název úlohy *Aktualizace na Windows 10*.

Krok 5. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Jak pozastavit ochranu nástrojem BitLocker pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Konfigurace obecných nastavení úlohy

Konfigurace obecných nastavení úlohy:

1. V rozevíracím seznamu **Application** vyberte **Kaspersky Endpoint Security**.
2. V rozevíracím seznamu **Task type** vyberte možnost **BitLocker protection management**.
3. Do pole **Task name** zadejte krátký popis, například *Aktualizace na Windows 10*.
4. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

Krok 2. Správa ochrany BitLocker

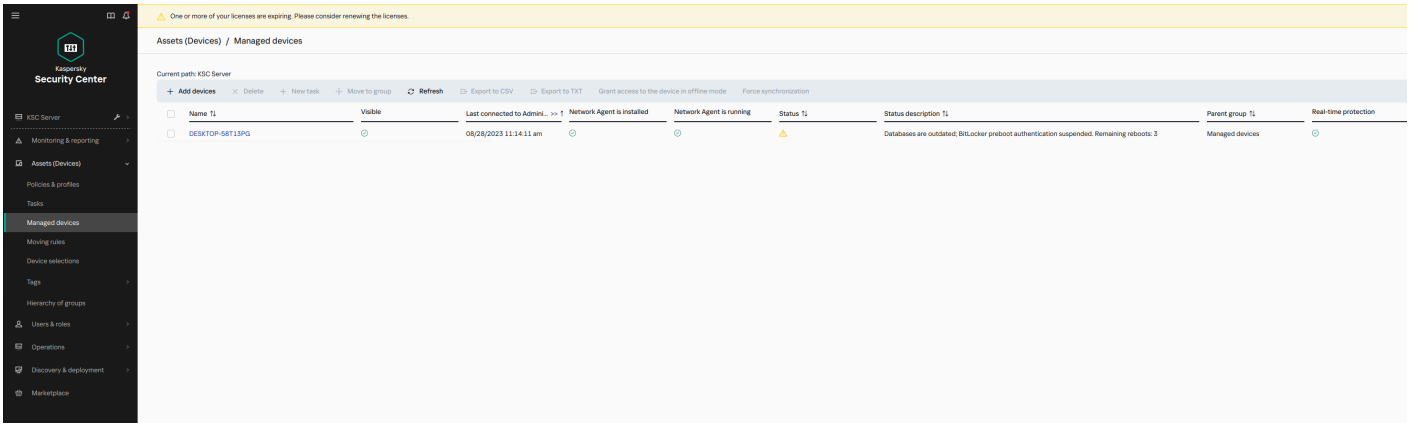
Konfigurace ověřování nástrojem BitLocker. Chcete-li pozastavit ochranu BitLocker, vyberte možnost **Temporarily allow skipping BitLocker authentication** a zadejte počet restartů bez ověření nástrojem BitLocker (1- až 15krát). V případě potřeby zadejte datum a čas vypršení platnosti úlohy. V uvedenou dobu se úloha automaticky vypne a uživatel musí po restartování počítače provést ověření BitLocker.

Krok 3. Dokončení vytvoření úlohy

Ukončete průvodce. V seznamu úloh se zobrazí nová úloha.

Chcete-li spustit úlohu, zaškrtněte políčko vedle úlohy a klikněte na tlačítko **Start**.

Když je úloha spuštěna, po dalším restartu počítače tak BitLocker nebude uživatele vyzývat k ověření. Po každém restartu počítače bez ověření nástrojem BitLocker vygeneruje aplikace Kaspersky Endpoint Security odpovídající událost a zaznamená počet zbývajících restartů. Kaspersky Endpoint Security poté odešle událost do Kaspersky Security Center, aby ji monitoroval správce. Počet zbývajících restartů také můžete zobrazit ve složce **Managed devices** konzoly aplikace Kaspersky Security Center v popisu stavu zařízení.



Seznam spravovaných zařízení

Když je dosaženo zadaného počtu restartů nebo doby vypršení platnosti úlohy, ověřování BitLocker se automaticky zapne. Aby uživatel získal přístup k datům, musí dokončit ověření nástrojem BitLocker.

Na počítačích se systémem Windows 7 nemůže BitLocker počítat restartování počítače. Počítání restartů na počítačích se systémem Windows 7 zajišťuje Kaspersky Endpoint Security. K automatickému zapnutí ověřování BitLocker po každém restartu je tedy nutné spustit aplikaci Kaspersky Endpoint Security.

Chcete-li zapnout ověřování nástrojem BitLocker předem, otevřete vlastnosti úlohy *Správa ochrany nástrojem BitLocker* a vyberte možnost **Žádat o ověření pokaždé před spuštěním**.

Šifrování na úrovni souborů na místních discích počítače

Šifrování souborů není podporováno na počítačích s architekturou ARM.

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

Kaspersky Endpoint Security nešifruje soubory, které jsou umístěny v cloudovém úložišti OneDrive nebo v jiných složkách, které mají název OneDrive. Kaspersky Endpoint Security také blokuje kopírování zašifrovaných souborů do složek OneDrive, pokud tyto soubory nejsou přidány do pravidla dešifrování.

Postup šifrování souborů na místních discích:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Data Encryption** → **File Level Encryption**.
4. V rozevíracím seznamu **Režim šifrování** vyberte možnost **Podle pravidel**.
5. 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**. Soubory ve standardní systémové složce *Oblíbené* 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.

        Nedoporučujeme šifrovat dočasné soubory, protože to může způsobit ztrátu dat. Například aplikace Microsoft Word vytváří při zpracování dokumentu dočasné soubory. Pokud jsou dočasné soubory zašifrovány, ale původní soubor nikoli, může se uživateli při pokusu o uložení dokumentu zobrazit chyba *Přístup odepřen*. Kromě toho může Microsoft Word soubor uložit, ale příště už nebude možné dokument otevřít, tj. data budou ztracena.

      - **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.
      - 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.
6. 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

Ve výchozím nastavení všechny aplikace pracují se šifrovanými soubory v dešifrovaném stavu. Pokud určité aplikace často používáte (například prohlížeče nebo textové editory), můžete za účelem ochrany informací vytvořit šifrovaná pravidla přístupu k souborům.

Pro prohlížeče Microsoft Internet Explorer a Microsoft Edge doporučujeme vytvořit pravidlo přístupu k šifrovanému souboru. Vzhledem k tomu, jak tyto prohlížeče fungují, se soubor automaticky dešifruje, pokud nahrajete šifrovaný soubor na web (například do cloudového úložiště). To může způsobit únik údajů. Pomocí těchto prohlížečů nelze nahrát šifrovaný soubor. Doporučujeme nastavit pravidlo **Udělit přístup pouze k šifrovaným souborům s šifrovaným textem**. Pro jiné prohlížeče (například Google Chrome) není nutné pravidlo vytvářet.

Postup vytvoření pravidel přístupu k šifrovaným souborům pro aplikace:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Data Encryption → File Level Encryption**.
4. V rozevíracím seznamu **Režim šifrování** vyberte možnost **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.

5. V pravé části okna vyberte kartu **Pravidla pro aplikace**.
6. 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 bloku **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.

   Podrobnosti o určitém pravidlu přístupu k šifrovaným souborům pro aplikaci se zobrazí v tabulce na kartě **Pravidla pro aplikace**.
7. 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.

Podrobnosti o určitém pravidlu přístupu k šifrovaným souborům pro aplikaci se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

8. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Data Encryption → File Level Encryption**.
4. V rozevíracím seznamu **Režim šifrování** vyberte možnost **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.

5. V pravé části okna vyberte kartu **Pravidla pro aplikace**.
6. 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 bloku **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 možnost **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.

   Informace o pravidle šifrování pro soubory vytvořené nebo upravené vybranými aplikacemi se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

7. 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 možnost **Šifrovat všechny vytvořené soubory**.

   Informace o pravidle šifrování pro soubory vytvořené nebo upravené vybranými aplikacemi se zobrazí v tabulce na kartě **Pravidla pro aplikace**.

8. Uložte změny.

Generování pravidla dešifrování

Postup generování pravidla dešifrování:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Data Encryption → File Level Encryption**.

4. V rozevíracím seznamu **Režim šifrování** vyberte možnost **Podle pravidel**.

5. 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.

6. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Data Encryption** → **File Level Encryption**.

4. V pravé části okna vyberte kartu **Šifrování**.

5. 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 **Odstranit** položku **Odstranit pravidlo a dešifrovat soubory**.

   Soubory a složky odebrané ze seznamu položek k šifrování jsou automaticky přidány na seznam položek k dešifrování.

6. Vytvořte seznam souborů k dešifrování.

7. 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Šifrování dat** → **Běžné nastavení šifrování**.

4. V bloku **Nastavení hesla** klikněte na tlačítko **Nastavení**.

5. Tím otevřete okno; v tomto okně vyberte kartu **Šifrované balíčky**.

6. Nakonfigurujte nastavení složitosti hesla při vytváření šifrovaných balíčků.

[Jak povolit kontrolu síly hesla při vytváření šifrovaných archivů ve webové konzole]

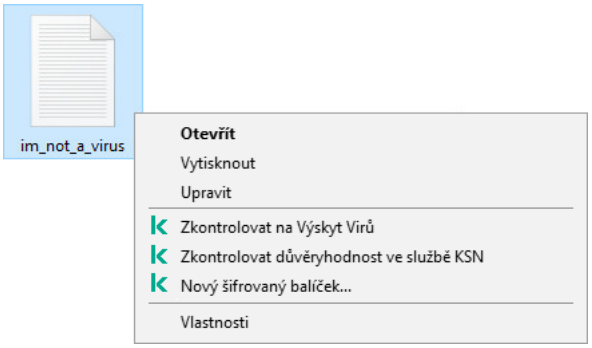
1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **File Level Encryption**.
5. V bloku **Encrypted package password settings** 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).



Vytvoření šifrovaného balíčku

3. V okně, které se otevře, zadejte heslo a potvrďte jej.
   Heslo musí splňovat kritéria složitosti uvedená v zásadě.
4. 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 –).

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.

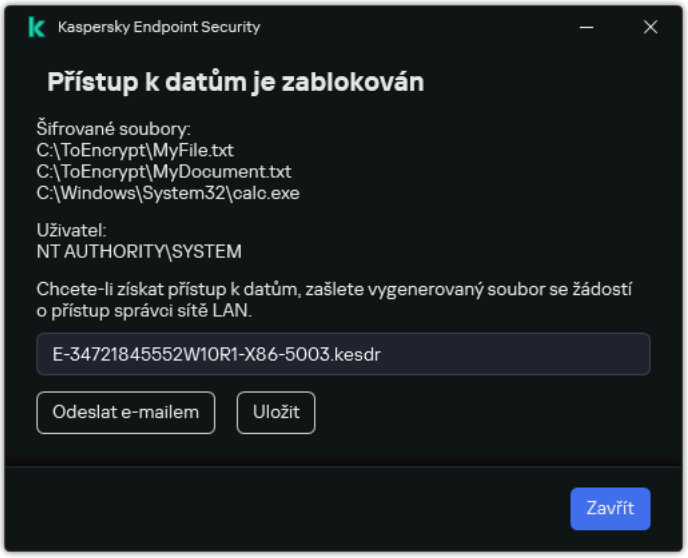
  Uživatel může se šifrovanými soubory pracovat za následujících okolností:

  - 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 přenosný 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

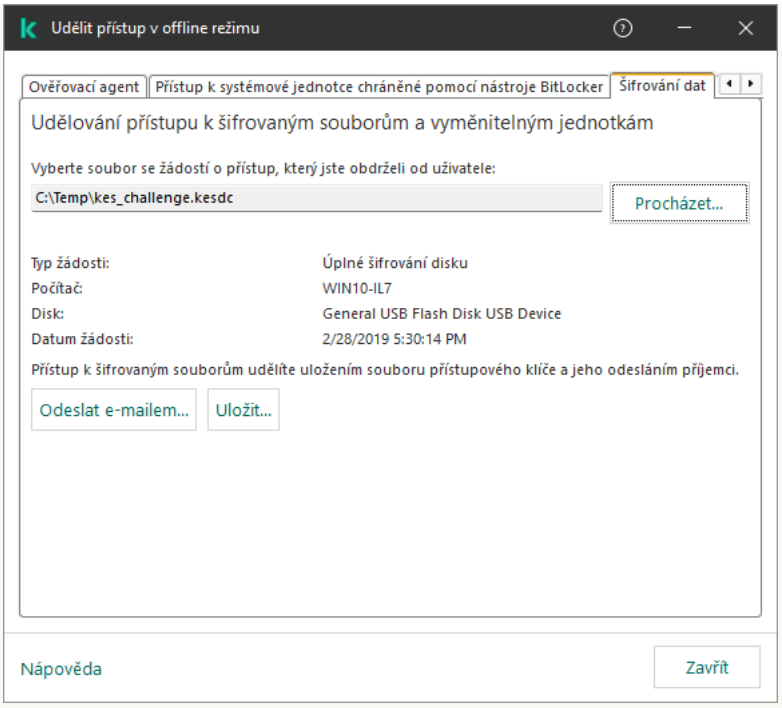
Chce-li uživatel zahájit proces obnovení, musí se pokusit o přístup k souboru. Aplikace Kaspersky Endpoint Security pak vytvoří soubor se žádostí o přístup (soubor s příponou KESDC), který uživatel musí zaslat správci, například e-mailem.

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 stromu konzoly vyberte možnost **Devices**.
3. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
4. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
5. Tím otevřete okno; v tomto okně vyberte kartu **Šifrování dat**.
6. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.
7. 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.



Udělit přístup v offline režimu

[Jak získat soubor klíče šifrovaného přístupu k datům ve webové konzole](#)

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.
3. Klikněte na tlačítko **Grant access to the device in offline mode**.
4. Vyberte možnost **Data Encryption**.
5. Klikněte na tlačítko **Select file** 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 **Save key** 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.

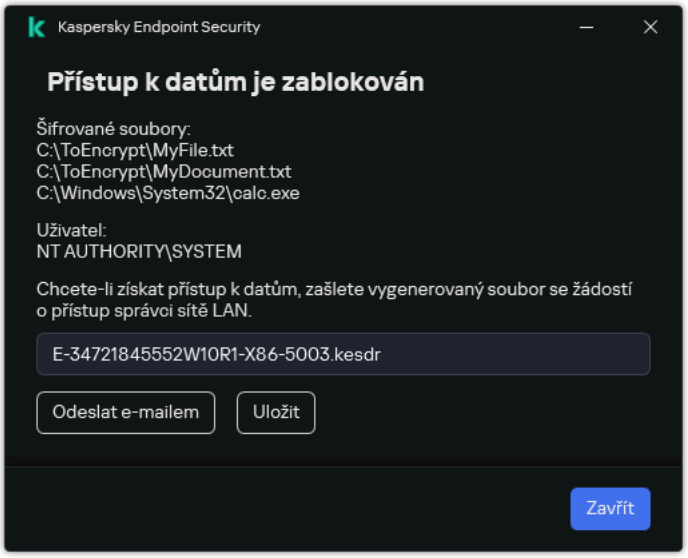
Úprava šablon zpráv pro přístup k šifrovaným souborům

Postup úpravy šablon zpráv pro přístup k šifrovaným souborům:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Běžné nastavení šifrování**.
4. V bloku **Šablony** klikněte na tlačítko **Šablony**.
5. V okně, které se otevře, postupujte takto:
   - Chcete-li upravit šablonu uživatelské zprávy, vyberte kartu **Zpráva uživatele**. Následující okno se otevře, když se uživatel pokusí o přístup k šifrovanému souboru a v počítači není k dispozici žádný klíč pro přístup k šifrovaným souborům (viz obrázek níže). Kliknutím na tlačítko **Odeslat e-mailem** automaticky vytvoříte zprávu uživatele. 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 **Zpráva správce**. Uživatel obdrží tuto zprávu po udělení přístupu k zašifrovaným souborům.
6. Upravte šablony zpráv.

   Chcete-li do textu šablony přidat proměnnou, umístěte kurzor na požadované místo, klikněte na možnost **Proměnná** a ze seznamu dostupných možností vyberte požadovanou proměnnou.

   Výchozí text šablony můžete také obnovit pomocí tlačítka **Výchozí režim**.
7. Uložte změny.



Blokování přístupu k šifrovaným souborům

Šifrování vyměnitelných jednotek

Šifrování vyměnitelných jednotek není podporováno na počítačích s architekturou ARM.

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:

- Full Disk Encryption (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).

- File Level Encryption (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 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.

Před šifrováním souborů na vyměnitelné jednotce se ujistěte, že je naformátovaná a že v ní nejsou žádné skryté oddíly (jako je systémový oddíl EFI). Pokud disk obsahuje neformátované nebo skryté oddíly, šifrování souborů může selhat s chybou.

Postup šifrování vyměnitelných jednotek:

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat → Šifrování vyměnitelných jednotek**.
4. V části **Režim šifrování** vyberte výchozí akci, kterou má aplikace Kaspersky Endpoint Security provádět na vyměnitelných jednotkách:
   - **Šifrovat celou vyměnitelnou jednotku** (FDE). 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.
5. Pokud chcete použít přenosný režim pro šifrování vyměnitelných jednotek, zaškrtněte políčko **Přenosný 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.
6. 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.
7. Pokud chcete nakonfigurovat šifrování pro jednotlivé vyměnitelné jednotky, definujte pravidla šifrování.
8. Jestliže chcete použít úplné šifrování disků vyměnitelných jednotek v režimu offline, zaškrtněte políčko **Povolit šifrování vyměnitelných jednotek 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 vyměnitelných jednotek v režimu offline** a není k dispozici žádné připojení k aplikaci Kaspersky Security Center, není šifrování vyměnitelné jednotky možné.
9. Uložte změny.

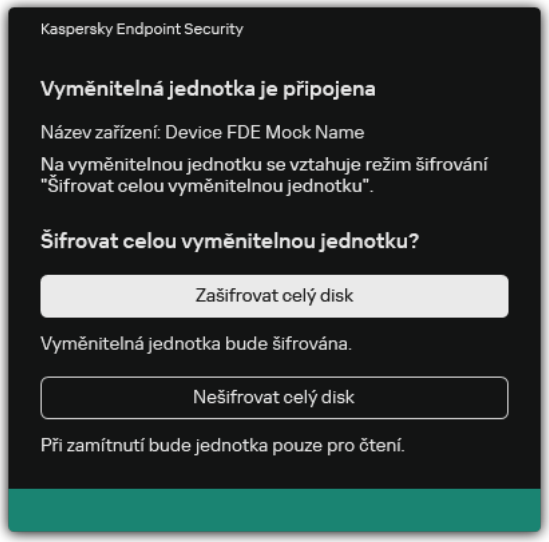
Jakmile po uplatnění zásady uživatel připojí vyměnitelnou jednotku nebo je-li vyměnitelná jednotka již připojena, aplikace Kaspersky Endpoint Security vyzve uživatele k potvrzení provedení šifrovací operace (viz obrázek níže).

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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
4. 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**.
5. V rozevíracím seznamu **Režim šifrování pro vybraná zařízení** vyberte akci, kterou má provést aplikace Kaspersky Endpoint Security se soubory na vybraných vyměnitelných jednotkách.
6. Zaškrtněte políčko **Přenosný 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.
7. 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 – 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.
8. 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 **Aktualizovat**.
9. 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. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Encryption of removable drives**.
5. V bloku **Encryption rules for selected devices** klikněte na odkaz **<N> rules**.
   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 **Export**.
   c. Potvrd'te, jestli chcete exportovat pouze vybraná pravidla, nebo exportovat celý seznam pravidel.
   d. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML ve výchozí složce pro stahování.
7. Postup importu seznamu pravidel:
   a. Klikněte na odkaz **Import**.
      V okně, které se otevře, vyberte soubor XML, ze kterého chcete importovat seznam pravidel.
   b. Otevřete soubor.
      Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.
8. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
4. 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. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje seznam pravidel do souboru XML.
5. 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. Otevřete soubor.

Pokud počítač již seznam pravidel obsahuje, aplikace Kaspersky Endpoint Security vás vyzve k odstranění stávajícího seznamu nebo k tomu, abyste k němu ze souboru XML přidali nové položky.

6. 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:

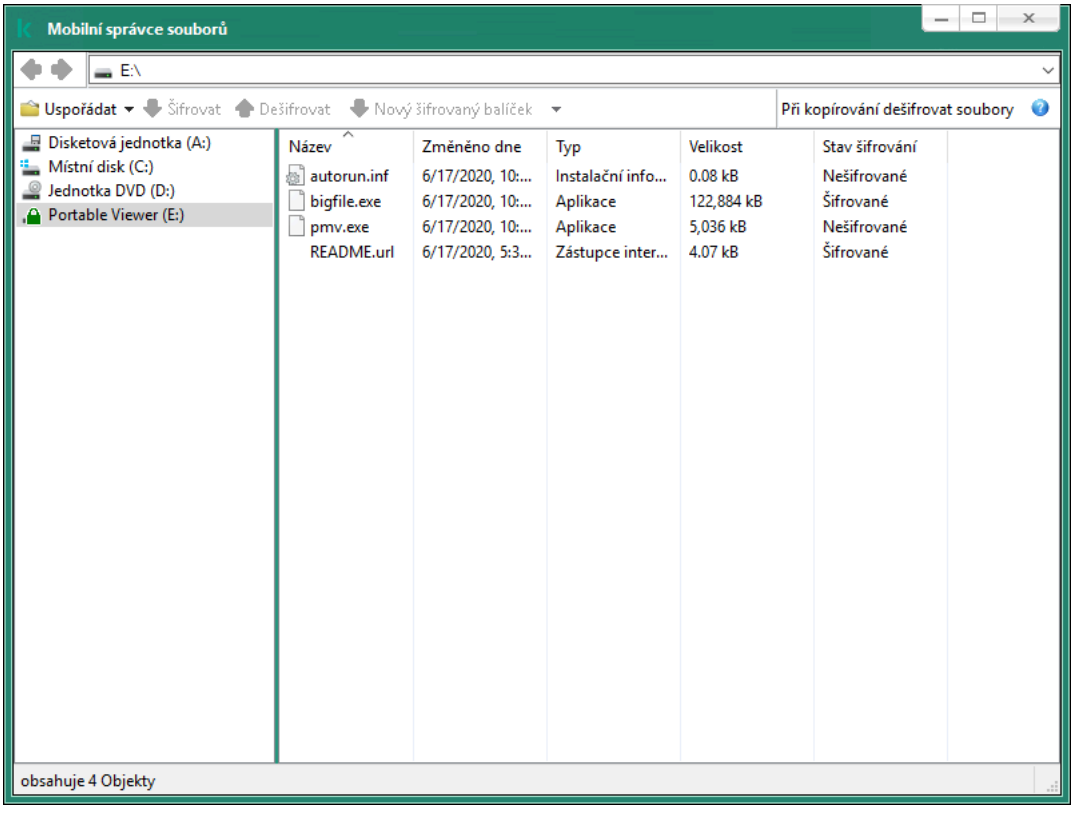
- Neexistuje žádné spojení mezi počítačem a serverem pro správu aplikace Kaspersky Security Center.
- Změnou serveru pro správu aplikace Kaspersky Security Center se změnila infrastruktura.
- V počítači není nainstalována aplikace Kaspersky Endpoint Security.

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

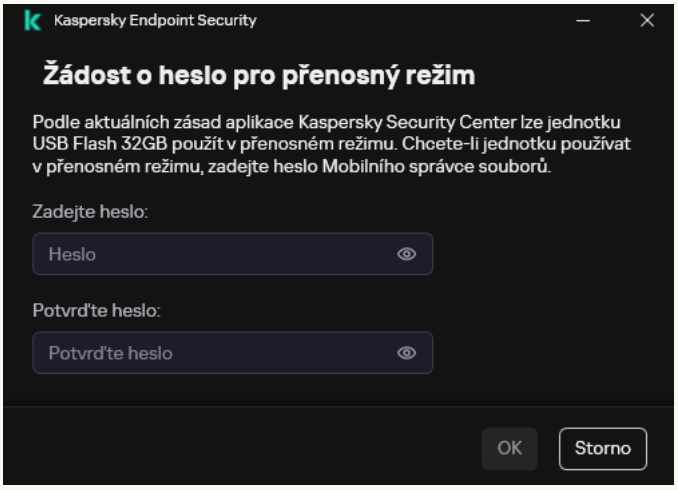
[Jak povolit podporu mobilního režimu pro práci se šifrovanými soubory na vyměnitelných jednotkách v konzole pro správu (MMC)]

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
4. V části **Režim šifrování pro vybraná zařízení** v rozevíracím seznamu vyberte **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).

5. Zaškrtněte políčko **Přenosný režim**.
6. V případě potřeby přidejte pravidla šifrování pro jednotlivé vyměnitelné jednotky.
7. Uložte změny.
8. Po použití zásad připojte vyměnitelnou jednotku k počítači.
9. Potvrďte operaci šifrování vyměnitelné jednotky.
   Otevře se okno, ve kterém můžete vytvořit heslo k Mobilnímu správci souborů.



Žádost o heslo pro přenosný režim

10. Zadejte heslo, které je dostatečně spolehlivé, a potvrďte jej.
11. Uložte změny.

Jak povolit podporu mobilního režimu pro práci se šifrovanými soubory na vyměnitelných jednotkách ve webové konzole

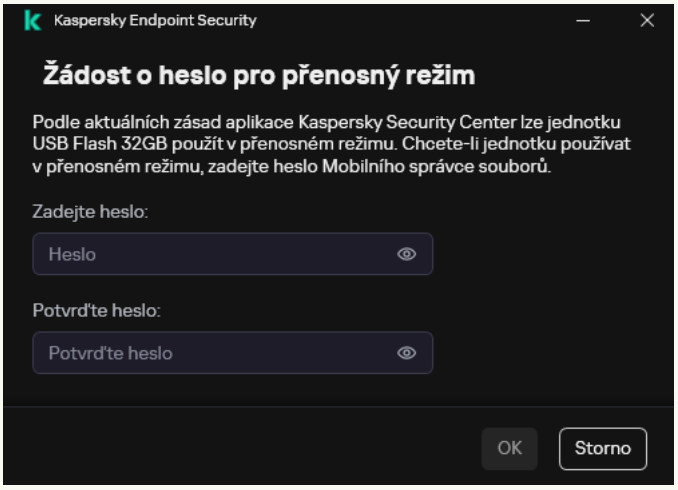
1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Data Encryption** → **Encryption of removable drives**.
5. V bloku **Default action** vyberte položku **Encrypt all files** nebo **Encrypt new files only**.

   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 **Portable mode**.
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.



Žádost o heslo pro přenosný režim

11. Zadejte heslo, které je dostatečně spolehlivé, a potvrďte jej.

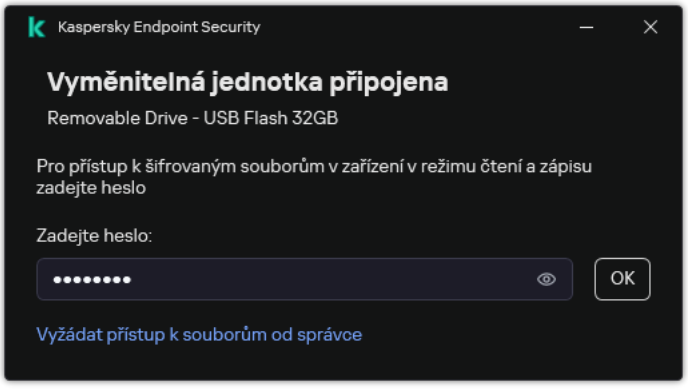
12. Uložte změny.

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 (viz obrázek níže).
- 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.



Přístup k šifrovaným souborům na vyměnitelné jednotce

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).

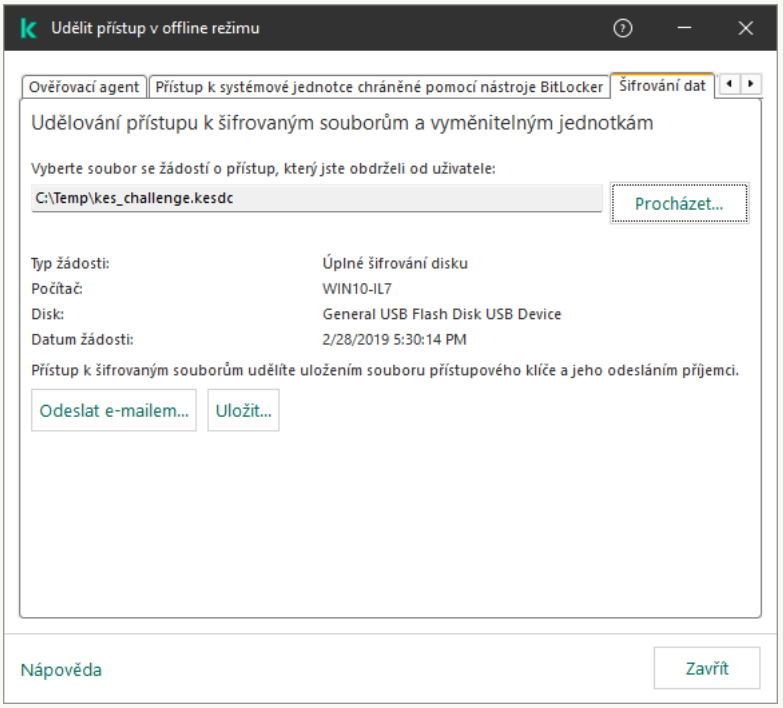
  Po dokončení procesu žádost–odpověď pro obnovení hesla získáte transparentní přístup k souborům na vyměnitelné jednotce a plný přístup k výměnné jednotce (oprávnění ke čtení a zápisu).

  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 stromu konzoly vyberte možnost **Devices**.
  3. Na kartě **Devices** vyberte počítač uživatele žádajícího o přístup k šifrovaným datům a kliknutím pravým tlačítkem myši otevřete kontextovou nabídku.
  4. V kontextové nabídce vyberte položku **Udělit přístup v offline režimu**.
  5. Tím otevřete okno; v tomto okně vyberte kartu **Šifrování dat**.
  6. Na kartě **Šifrování dat** klikněte na tlačítko **Procházet**.
  7. 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.



Udělit přístup v offline režimu

Jak získat soubor šifrovaného přístupu k datům ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Zaškrtněte políčko vedle názvu počítače, k jehož datům chcete obnovit přístup.
3. Klikněte na tlačítko **Grant access to the device in offline mode**.
4. Vyberte možnost **Data Encryption**.
5. Klikněte na tlačítko **Select file** 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 **Save key** 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. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Šifrování dat** → **Šifrování vyměnitelných jednotek**.
4. Pokud chcete dešifrovat všechny šifrované soubory uložené na vyměnitelných jednotkách, vyberte z rozevíracího seznamu **Režim šifrování** položku **Dešifrovat celou vyměnitelnou jednotku**.
5. 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.
   c. V místní nabídce tlačítka **Nastavit pravidlo** vyberte položku **Dešifrovat celou vyměnitelnou jednotku**.
6. 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.

Zobrazení stavu šifrování

Můžete se podívat na stav a sledovat šifrování dat. Aplikace Kaspersky Endpoint Security přiřazuje následující stavy šifrování:

- **Does not meet the policy; canceled by user**. Uživatel zrušil šifrování dat.

- **Does not meet the policy due to an error**. Chyba šifrování dat, například kvůli chybějící licenci.
- **Applying the policy; restart is required**. V počítači probíhá šifrování dat. Šifrování dat dokončíte restartováním počítače.
- **No encryption policy specified**. Šifrování dat je vypnuto v nastavení zásad.
- **Not supported**. V počítači nejsou nainstalovány součásti šifrování dat.
- **Applying the policy**. V počítači probíhá šifrování a/nebo dešifrování dat.

Postup zobrazení stavu šifrování dat počítače:

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Managed devices**.
3. V pracovním prostoru na kartě **Devices** přesuňte posuvník zcela vpravo. Pokud se **Encryption status** nezobrazuje, přidejte tento sloupec do nastavení konzoly aplikace Kaspersky Security Center.

   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.
4. Pokud je stav šifrování dat u počítače **Applying policy**, můžete sledovat panel průběhu šifrování:
   a. Dvojitým kliknutím otevřete vlastnosti počítače **Applying policy**.
   b. V okně vlastností počítače vyberte část **Applications**.
   c. V seznamu aplikací Kaspersky nainstalovaných v počítači vyberte **Kaspersky Endpoint Security for Windows**.
   d. Klikněte na tlačítko **Statistics**.
   e. V části **Encryption of devices** vidíte aktuální průběh šifrování dat v procentech.

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 konzoly vyberte uzel **Administration Server**.
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**.
   b. V okně, které se otevře, klikněte na tlačítko **Add**.
   c. Otevře se okno; v tomto okně zadejte do části **General** název stránky.
   d. V části **Information panels** klikněte na tlačítko **Add**.
   e. V okně, které se otevře ve skupině **Protection status**, vyberte položku **Encryption of devices**.
   f. Klikněte na tlačítko **OK**.
   g. V případě potřeby upravte nastavení podokna podrobností. To provedete v částech **View** a **Devices**.
   h. Klikněte na tlačítko **OK**.
   i. Opakujte kroky s pokyny d–h a v části **Protection status** vyberte položku **Encryption of removable drives**.
   Přidaná podokna podrobností se zobrazí v seznamu **Information panels**.
   j. Klikněte na tlačítko **OK**.
   Název stránky s podokny podrobností vytvořenými v předchozím kroku se zobrazí v seznamu **Pages**.
   k. 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 stromu konzoly vyberte možnost **Managed devices**.
3. Na kartě **Devices** vyberte ze seznamu název počítače a kliknutím pravým tlačítkem myši otevřete místní nabídku.
4. V kontextové nabídce počítače vyberte položku **Properties**. V okně, které se otevře, vyberte část **Protection**.
5. Kliknutím na odkaz **View data encryption errors** otevřete 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

Aplikace Kaspersky Security Center vám umožňuje vytvářet zprávy o šifrování dat:

- **Report on encryption status of managed devices**. Zpráva obsahuje informace o tom, zda stav šifrování počítače odpovídá zásadám šifrování.
- **Report on encryption status of mass storage devices**. Zpráva obsahuje informace o stavu šifrování externích zařízení a úložných zařízení.
- **Report on rights to access encrypted drives**. Zpráva obsahuje informace o stavu účtů, které mají přístup k šifrovaným jednotkám.
- **Report on file encryption errors**. Zpráva obsahuje informace o chybách, ke kterým došlo při provádění úloh šifrování nebo dešifrování dat na počítačích.
- **Report on blockage of access to encrypted files**. Zpráva obsahuje informace o aplikacích, kterým je blokován přístup k zašifrovaným souborům.

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 New Report Template Wizard.
4. Postupujte podle pokynů průvodce Report Template Wizard. V okně **Selecting the report template type** v části **Other** vyberte jednu ze zpráv o šifrování dat.

   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.

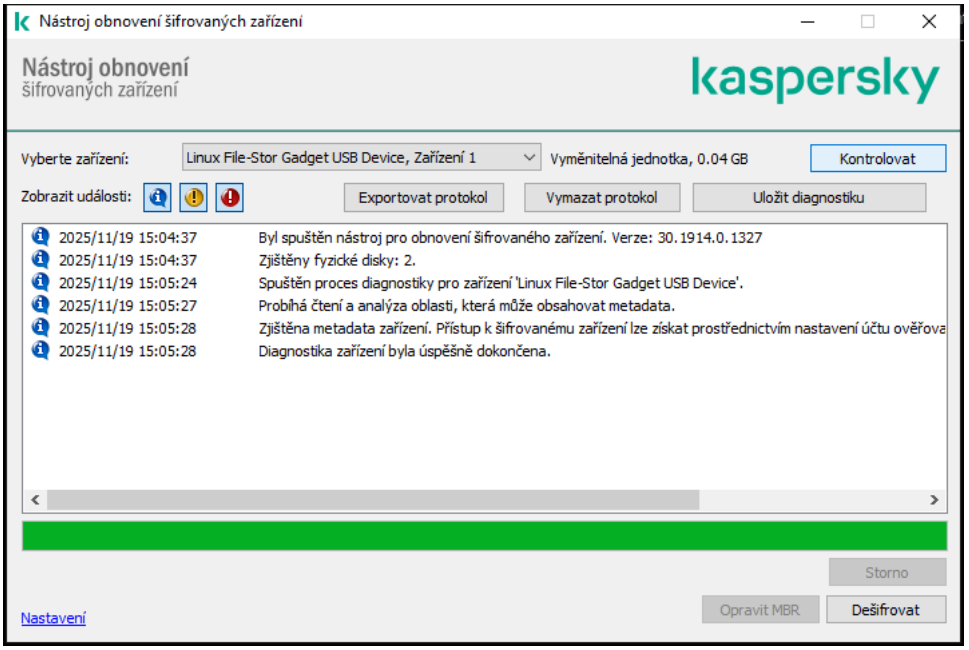
Před obnovením dat v šifrovaných zařízeních se doporučuje zrušit zásady aplikace Kaspersky Security Center nebo zakázat šifrování v nastavení zásad aplikace Kaspersky Security Center v počítači, ve kterém bude proveden postup. Tím předejdete opětovnému šifrování zařízení.

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 .
2. V okně, které se otevře, klikněte na tlačítko **Obnovení šifrování 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 Nástroj pro obnovení vyberte šifrované zařízení, ke kterému chcete obnovit přístup.
3. Kliknutím na tlačítko **Kontrolovat** 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 konzoly pro správu vyberte možnosti **Advanced** → **Data encryption and protection** → složku **Encrypted drives**.
3. Vyberte v pracovním prostoru šifrované zařízení, pro které chcete vytvořit soubor přístupového klíče, a v kontextové nabídce zařízení klikněte na **Přístup k zařízení můžete získat v produktu Kaspersky Endpoint Security**.

   Pokud si nejste jistí, pro který počítač byl soubor s žádostí o přístup vygenerován, vyberte ve stromu konzoly pro správu složku **Advanced** → **Data encryption and protection** a v pracovním prostoru klikněte na položku **Šifrovací klíč k zařízení můžete získat v produktu Kaspersky Endpoint Security**.

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: *Strong encryption (AES256)* nebo *Lite encryption (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.

5. Kliknutím na tlačítko **Procházet** otevřete okno; v tomto okně zadejte cestu k souboru žádosti s příponou fdertc přijatého od uživatele.
6. Klikněte na tlačítko **Odemknout**.

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 **Operations** → **Data encryption and protection** → **Encrypted drives**.
2. Zaškrtněte políčko vedle názvu počítače, na němž chcete obnovit data.
3. Klikněte na tlačítko **Grant access to the device in offline mode**.

   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: *Strong encryption (AES256)* nebo *Lite encryption (AES56)*. Knihovna šifrování AES se instaluje společně s aplikací.

   c. Vyberte soubor se žádostí o přístup, který jste obdrželi od uživatele (soubor s příponou FDERTC).
   d. Vyberte složku, do které chcete uložit soubor klíče šifrovaného přístupu 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).

Řešení Detection and Response

Řešení Kaspersky Detection and Response jsou bezpečnostní systémy pro detekci pokročilých hrozeb a indikátorů útoku na různých úrovních infrastruktury organizace. Řešení Detection and Response poskytují informace o detekované hrozbě a umožňují spravovat akce součásti Reakce na hrozby.

Řešení Detection and Response tedy dělají následující:

- Přijímají informace o provozu počítače, serveru nebo jiných zařízení (telemetrie).
- Automaticky analyzují informace k detekci hrozeb.
- Generují podrobnosti o výstraze jako sloupce řetězce vývoje hrozby pro analýzu a výběr akcí součásti Reakce na hrozby.
- Provádějí akce součásti Reakce na hrozby (například izolace počítače od sítě).

Kaspersky Endpoint Security podporuje řešení Detection and Response pomocí integrovaného agenta. Integrovaný agent posílá telemetrii na servery řešení a provádí akce součásti Reakce na hrozby. Integrovaný agent podporuje:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) verze 7.1 nebo starší
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premise)
- Kaspersky Sandbox 2.0

Aplikaci Kaspersky Endpoint Security můžete používat s řešením Detection and Response v různých konfiguracích, např. [EDR Optimum+MDR].

Licence k MDR a EDR Optimum

Kaspersky Endpoint Security podporuje funkce řešení Kaspersky Managed Detection and Response (MDR) a Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Kaspersky Endpoint Security můžete s těmito řešeními používat v různých konfiguracích a vytvořit si vlastní systém ochrany, který splní vaše konkrétní požadavky. Chcete-li tak učinit, musíte si zakoupit licenci pro každé z těchto řešení. Licence může zahrnovat právo používat jedno řešení (například pouze doplněk MDR) nebo více řešení, doplněk [EDR Optimum+MDR].

MDR a EDR Optimum podporují následující způsoby licencování:

- Funkce MDR nebo EDR Optimum je součástí licence k aplikaci Kaspersky Endpoint Security pro systém Windows.

  Tato funkce je k dispozici okamžitě po aktivaci aplikace Kaspersky Endpoint Security pro systém Windows. Stačí přidat jeden klíč.

- Samostatná licence pro MDR nebo EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Funkce bude dostupná po přidání samostatného klíče pro doplněk MDR, doplněk EDR Optimum nebo doplněk [EDR Optimum+MDR]. V počítači tak jsou přidány dva klíče: klíč pro aplikaci Kaspersky Endpoint Security a klíč pro MDR nebo EDR Optimum. Klíč k aplikaci Kaspersky Endpoint Security musí být přidán jako první.

Kaspersky Endpoint Security umožňuje přidat pouze jeden *aktivní klíč* pro licencování MDR a EDR Optimum. Pokud tedy potřebujete aktivovat obě tato řešení, musíte místo samostatného klíče pro každé řešení přidat jeden doplňkový klíč pro [EDR Optimum+MDR] Add-on. Můžete také jeden *rezervní klíč*.

Pokud jste při nasazení MDR použili soubor BLOB, nepotřebujete k aktivaci MDR samostatný klíč. Soubor BLOB již obsahuje informace o licenci.

Počáteční licencování řešení

Při prvním nasazení MDR a EDR Optimum se řešení aktivují stejným způsobem jako aplikace Kaspersky Endpoint Security. Klíč můžete přidat pomocí úlohy *Přidání klíče* nebo použijte funkci automatické distribuce klíčů. Licenční klíč je přidán do aplikace jako druhý aktivní klíč nebo jako rezervní klíč, pokud zaškrtnete příslušné políčko.

Přechod z jedné licence na druhou

Pokud vaše organizace již má jedno z těchto řešení nasazeno a odpovídající klíč byl přidán do aplikace, je potřeba v souvislosti s licencováním nové konfigurace vzít v úvahu určité aspekty. Při přechodu na jinou licenci aplikace nový klíč do aplikace nepřidá, ale nahradí aktuální klíč novým klíčem. Důvodem je omezení, které aplikaci umožňuje přidat pouze jeden klíč pro aktivaci MDR a EDR Optimum.

Předpokládejme například, že vaše organizace má nasazené řešení [EDR Optimum+MDR] a vy jste se rozhodli přejít na konfiguraci s doplňkem MDR. Chcete-li přejít na novou konfiguraci, musíte vyměnit klíč k doplňku [EDR Optimum+MDR] Add-on Optimum+MDR] za klíč k doplňku MDR.

Samostatná licence pro EDR Optimum a MDR (doplněk [EDR Optimum+MDR]) již není k dispozici. Pokud chcete používat obě tato řešení, musíte aktivovat MDR pomocí souboru BLOB a EDR Optimum pomocí licenčního klíče.

Díky funkci automatické distribuce klíčů aplikace odmítá licenční klíče, které pokrývají stejný počet řešení. To znamená, že pokud máte přidán klíč k doplňku EDR Optimum, nemůžete tento klíč nahradit klíčem k doplňku MDR. Klíč k doplňku EDR Optimum však můžete nahradit klíčem k doplňku [EDR Optimum+MDR]. Aplikace také odmítne klíče, pokud se pokusíte nahradit klíč k doplňku MDR klíčem k doplňku EDR. Chcete-li vyměnit klíč, můžete spustit úlohu *Přidání klíče*. Úloha *Přidání klíče* umožňuje nahradit licenční klíče libovolným počtem řešení.

Pokud máte přidaný rezervní klíč k doplňku [EDR Optimum+MDR] Add-on, pro správné přidání aktivního klíče k doplňku EDR Optimum nebo MDR musíte nejprve vyměnit rezervní klíč za klíč k doplňku EDR Optimum nebo MDR, případně odeberte rezervní klíč a poté vyměňte aktivní klíč.

Kompatibilita s řešeními EDR třetích stran

Kaspersky Endpoint Security můžete použít k ochraně pracovních stanic a serverů společně s řešeními EDR třetích stran. Chcete-li eliminovat falešně pozitivní výsledky, doporučujeme přidat spustitelné soubory aplikace Kaspersky Endpoint Security a Network Agent do důvěryhodné zóny vašeho řešení EDR třetí strany.

Důvěryhodná zóna pro kompatibilitu s řešeními EDR třetích stran

	Kaspersky Endpoint Security pro systém Windows	Kaspersky Security Center Network Agent
Pracovní složka	`C:\Program Files (x86)\Kaspersky Lab\KES.14.0.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Spustitelné soubory	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`

```
klshwmsg.exe
klwd.exe
ksnproxy.exe
Patch.exe
tslauncher.exe
Up2Date.exe
vapm.exe
```

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent 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.

Chcete-li používat Kaspersky Endpoint Agent jako součást řešení Kaspersky, musíte tato řešení aktivovat pomocí příslušného licenčního klíče.

Úplné informace o aplikaci Kaspersky Endpoint Agent obsažené v softwarovém řešení, které používáte, a úplné informace o samostatném řešení naleznete v příručce nápovědy k příslušnému produktu:

- Nápověda k platformě Kaspersky Anti Targeted Attack Platform
- Nápověda k aplikaci Kaspersky Sandbox
- Nápověda k aplikaci Kaspersky Endpoint Detection and Response Optimum
- Nápověda k aplikaci Kaspersky Managed Detection and Response

Distribuční sada pro aplikaci Kaspersky Endpoint Security verze 11.2.0–11.8.0 obsahuje aplikaci Kaspersky Endpoint Agent. Aplikaci Kaspersky Endpoint Agent můžete vybrat při instalaci aplikace Kaspersky Endpoint Security pro systém Windows. Na váš počítač tak budou nainstalovány dvě aplikace: KEA a KES. V aplikaci Kaspersky Endpoint Security 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady Kaspersky Endpoint Security.

Korespondence verzí KEA (jako součásti KES) s verzemi KES

Kaspersky Endpoint Security pro systém Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Společnost Kaspersky všechna řešení Detection and Response převádí tak, aby fungovala s integrovaným agentem Kaspersky Endpoint Security namísto aplikace Kaspersky Endpoint Agent. Kaspersky postupně přidává podporu pro tato řešení a postupně vyřazuje Kaspersky Endpoint Agent (viz tabulku níže). Počínaje verzí 12.1 aplikace podporuje všechna řešení Detection and Response. Kromě toho od verze 12.1 navíc aplikace již není kompatibilní s Kaspersky Endpoint Agent a instalace obou aplikací vedle sebe na stejný počítač již není možná.

Nasazení integrovaného agenta pro správu řešení Detection and Response

Verze aplikace Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (součást Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (součást Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent

11.8.0	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	Kaspersky Endpoint Agent
12.6	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**	**Integrovaný agent**

Migrace konfigurace [KES+KEA] na konfiguraci [KES+integrovaný agent]

Součástí aplikace Kaspersky Endpoint Security jsou integrovaní agenti pro práci s řešeními Detection and Response. Pro práci s těmito řešeními už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent. Když nasadíte Kaspersky Endpoint Security do počítačů s nainstalovanou aplikací Kaspersky Endpoint Agent, řešení Detection and Response budou nadále fungovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent.

Distribuční sada pro aplikaci Kaspersky Endpoint Security verze 11.2.0–11.8.0 obsahuje aplikaci Kaspersky Endpoint Agent. Aplikaci Kaspersky Endpoint Agent můžete vybrat při instalaci aplikace Kaspersky Endpoint Security pro systém Windows. Na váš počítač tak budou nainstalovány dvě aplikace: KEA a KES. V aplikaci Kaspersky Endpoint Security 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady Kaspersky Endpoint Security.

Migrace konfigurace [KES+KEA] do konfigurace [KES+integrovaný agent] zahrnuje následující kroky:

1. **Upgrade aplikace Kaspersky Security Center**

   Upgradujte všechny součásti aplikace Kaspersky Security Center na verzi 13.2 nebo novější, včetně součásti Network Agent na uživatelských počítačích a webové konzoly.

2. **Upgrade webového pluginu Kaspersky Endpoint Security**

   Ve webové konzole Kaspersky Security Center upgradujte webový plugin aplikace Kaspersky Endpoint Security na verzi 11.7.0 nebo novější. Ke správě součástí EDR Optimum a Kaspersky Sandbox musíte používat webovou konzolu.

   Chcete-li používat Kaspersky Anti Targeted Attack Platform (EDR), budete potřebovat webový modul plug-in pro Kaspersky Endpoint Security verze 12.1 nebo novější.

   Chcete-li používat Kaspersky Anti Targeted Attack Platform (NDR), budete potřebovat webový modul plug-in pro Kaspersky Endpoint Security verze 12.7 nebo novější.

3. **Migrace zásady a úkolů**

   Nastavení aplikace Kaspersky Endpoint Agent můžete migrovat na aplikaci Kaspersky Endpoint Security pro systém Windows pomocí průvodce migrací zásad aplikace Kaspersky Endpoint Agent.

   Tento postup vytvoří novou zásadu aplikace Kaspersky Endpoint Security. Nová zásada má stav *Inactive*. Chcete-li novou zásadu použít, otevřete vlastnosti zásady, přijměte Prohlášení o Kaspersky Security Network a nastavte stav na *Active*.

4. **Jak funguje licence**

   Pokud používáte k aktivaci aplikací Kaspersky Endpoint Security pro systém Windows a Kaspersky Endpoint Agent společnou licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security, funkce EDR Optimum bude aktivována automaticky po upgradu aplikace na verzi 11.7.0. Nemusíte dělat nic jiného.

   Jestliže používáte k aktivaci funkce EDR Optimum licenci k doplňku Kaspersky Endpoint Detection and Response Optimum, do úložiště aplikace Kaspersky Security Center se přidá klíč k doplňku EDR Optimum je povolena automatická distribuce licenčního klíče. Po upgradu aplikace na verzi 11.7.0 je funkce EDR Optimum aktivována automaticky.

   Pokud používáte k aktivaci aplikace Kaspersky Endpoint Agent licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security a jinou licenci k aktivaci Kaspersky Endpoint Security pro systém Windows, musíte nahradit klíč k aplikaci Kaspersky Endpoint Security pro systém Windows společným klíčem k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security. Klíč můžete nahradit pomocí úlohy *Add key*.

   Nemusíte aktivovat funkci Kaspersky Sandbox. Funkce Kaspersky Sandbox bude k dispozici okamžitě po upgradu a aktivaci aplikace Kaspersky Endpoint Security pro systém Windows.

   K aktivaci aplikace Kaspersky Endpoint Security jako součásti řešení Kaspersky Anti Targeted Attack Platform lze použít pouze licenci k řešení Kaspersky Anti Targeted Attack Platform. Po upgradu aplikace na verzi 12.1 je funkce EDR (KATA) aktivována automaticky. Nemusíte dělat nic jiného.

5. **Upgrade aplikace Kaspersky Endpoint Security**

   Chcete-li upgradovat aplikaci a migrovat funkci EDR Optimum a Kaspersky Sandbox, doporučujeme úlohu vzdálené instalace.

   Pro upgrade aplikace pomocí úlohy vzdálené instalace musíte upravit následující nastavení:

   - V nastavení instalačního balíčku vyberte součásti pro řešení Detection and Response.
   - V nastavení instalačního balíčku (pro Kaspersky Endpoint Security pro Windows verze 11.2.0–11.8.0) vylučte součást Kaspersky Endpoint Agent.
   - Pokud je povolena ochrana heslem pro omezení přístupu k aplikaci Kaspersky Endpoint Agent, zadejte heslo pro odinstalaci aplikace v nastavení úlohy *Install application remotely*. Heslo pro odinstalaci můžete zadávat od verze aplikace Kaspersky Security Center Linux 15.1.

   Aplikaci můžete také upgradovat následujícími způsoby:

   - Pomocí aktualizační služby Kaspersky (Seamless Update – SMU).
   - Místně pomocí průvodce instalací.

   Aplikace Kaspersky Endpoint Security podporuje automatický výběr součástí při upgradu aplikace na počítači, na němž je nainstalována aplikace Kaspersky Endpoint Agent. Automatický výběr součástí závisí na oprávněních uživatelského účtu, který aplikaci upgraduje.

   Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru EXE nebo MSI pod systémovým účtem (SYSTEM), Kaspersky Endpoint Security získá přístup k aktuálním licencím řešení Kaspersky. Pokud je tedy v počítači nainstalována například aplikace Kaspersky Endpoint Agent a aktivováno řešení EDR Optimum, instalační program aplikace Kaspersky Endpoint Security automaticky nakonfiguruje sadu součástí a vybere součást EDR Optimum. Tím se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent. Spuštění instalačního programu MSI pod systémovým účtem (SYSTEM) se obvykle provádí při upgradu prostřednictvím aktualizační služby Kaspersky (SMU) nebo při nasazování instalačního balíčku prostřednictvím aplikace Kaspersky Security Center.

   Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru MSI pod uživatelským účtem bez oprávnění, Kaspersky Endpoint Security nemá přístup k aktuálním licencím řešení Kaspersky. V tomto případě Kaspersky Endpoint Security automaticky vybere součásti na základě konfigurace Kaspersky Endpoint Agent. Poté se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent.

6. **Restart počítače**

   Restartujte počítač a dokončete aktualizaci aplikace pomocí integrovaného agenta. Při upgradu aplikace instalátor před restartováním počítače odstraní aplikaci Kaspersky Endpoint Agent. Po restartování počítače instalátor přidá integrovaného agenta. To znamená, že aplikace Kaspersky Endpoint Security neprovádí funkce EDR a Kaspersky Sandbox, dokud není počítač restartován.

7. **Kontrola stavu řešení Kaspersky Endpoint Detection and Response Optimum a Kaspersky Sandbox**

   Pokud je po upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

   - Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
   - Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*.
   - V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.
   - Pomocí *Report on status of application components* zkontrolujte, zda je aktivována funkce EDR Optimum. Pokud je stav součásti *Není součástí licence*, zkontrolujte, zda je u EDR Optimum zapnuta funkce automatické distribuce licenčního klíče.

Migrace zásad a úloh pro Kaspersky Endpoint Agent

Aplikace Kaspersky Endpoint Security pro Windows průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security. Migrovat lze nastavení zásad a úloh pro následující řešení:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security funguje pouze ve webové konzole a cloudové konzole. V konzole pro správu (MMC) můžete nastavení pro řešení Kaspersky Anti Targeted Attack Platform (EDR) migrovat pouze pomocí standardního průvodce migrací zásad a úloh aplikace Kaspersky Security Center.

Doporučujeme začít s migrací Kaspersky Endpoint Agent na Kaspersky Endpoint Security na jednom počítači, poté ji provést na skupině počítačů a poté dokončit migraci na všech počítačích organizace.

Chcete-li migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security,

v hlavním okně webové konzoly vyberte možnost **Operations → Migration from Kaspersky Endpoint Agent**.

Tím spustíte průvodce migrací zásad a úloh. Postupujte podle pokynů průvodce.

Krok 1. Migrace zásad

Průvodce migrací vytvoří novou zásadu, která sloučí nastavení zásad aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete sloučit se zásadami aplikace Kaspersky Endpoint Security. Kliknutím na zásadu aplikace Kaspersky Endpoint Agent vyberte zásadu aplikace Kaspersky Endpoint Security, s níž chcete sloučit nastavení. Zkontrolujte, zda jste vybrali správné zásady, a přejděte k dalšímu kroku.

Krok 2. Migrace úloh

Nové úlohy pro aplikaci Kaspersky Endpoint Security vytvoří průvodce migrací. V seznamu úloh vyberte úlohy aplikace Kaspersky Endpoint Agent, které chcete vytvořit pro zásady aplikace Kaspersky Endpoint Security. Průvodce podporuje úlohy pro řešení Kaspersky Endpoint Detection and Response a Kaspersky Sandbox. Přejděte k dalšímu kroku.

Krok 3. Dokončení průvodce

Ukončete průvodce. Průvodce tak provede následující:

- Vytvoří novou zásadu aplikace Kaspersky Endpoint Security.

  V zásadě se sloučí nastavení z aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Název zásady je *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Nová zásada má stav *Inactive*. Chcete-li pokračovat, změňte stav zásad aplikací Kaspersky Endpoint Agent a Kaspersky Endpoint Security na *Inactive* a aktivujte novou sloučenou zásadu.

  Po migraci z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security pro systém Windows zkontrolujte, zda má nová zásada nastavenu funkci přenosu dat na server pro správu (data souborů v karanténě a údaje o řetězci vývoje hrozeb). Hodnoty parametrů přenosu dat nejsou ze zásady aplikace Kaspersky Endpoint Agent migrovány.

  Při migraci z aplikace Kaspersky Endpoint Agent na řešení Kaspersky Endpoint Security pro řešení Kaspersky Anti Targeted Attack Platform (EDR) může dojít k chybám při připojování počítače k serverům součásti Central Node. Důvodem je, že průvodce migrací ve webové konzole přeskočí následující nastavení zásad a nemigruje je:

  - Zákaz změny nastavení **Connection to KATA servers** („zámek").

    Ve výchozím nastavení lze nastavení měnit („zámek" je otevřený). Nastavení se proto v počítači nepoužijí. Musíte zakázat změnu nastavení a „zámek" zavřít.

  - Kryptokontejner.

    Pokud pro připojení k serverům Central Node používáte obousměrné ověřování, musíte znovu přidat kryptokontejner. Průvodce migrací správně migruje certifikát serveru TLS.

  Průvodce migrací zásad a úloh v konzole pro správu (MMC) migruje všechna nastavení řešení Kaspersky Anti Targeted Attack Platform (EDR).

- Vytvoří nové úlohy aplikace Kaspersky Endpoint Security.

  Nové úlohy jsou kopie úloh aplikace Kaspersky Endpoint Agent pro řešení Kaspersky Endpoint Detection and Response a Kaspersky Sandbox. Zároveň ponechá průvodce úlohy aplikace Kaspersky Endpoint Agent beze změny.

Jak migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security v konzole pro správu (MMC) (pouze u KATA (EDR))

1. V konzole pro správu vyberte položku Administration Server a kliknutím pravým tlačítkem otevřete místní nabídku.
2. Vyberte **All tasks → Policies and tasks batch conversion wizard**.

Spustí se průvodce hromadným převodem zásad a úloh. Postupujte podle pokynů průvodce.

Krok 1. Výběr aplikace, pro kterou potřebujete převést zásady a úlohy

V tomto kroku musíte vybrat Kaspersky Endpoint Security pro systém Windows. Přejděte k dalšímu kroku.

Krok 2. Převod zásad

Průvodce migrací vytvoří novou zásadu aplikace Kaspersky Endpoint Security, do které budou migrována nastavení zásad aplikace Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete převést do zásady aplikace Kaspersky Endpoint Security. Přejděte k dalšímu kroku.

Průvodce migrací poté začne převádět zásady. Během převodu zásad vás průvodce migrací vyzve, abyste přijali prohlášení o Kaspersky Security Network. Nové zásady budou mít název *<Název zásady> (converted)*.

Krok 3. Převod úloh

Tento krok přeskočte. Průvodce podporuje pouze úlohy pro řešení Kaspersky Endpoint Detection and Response Optimum a Kaspersky Sandbox. Správa těchto součástí je dostupná pouze ve webové konzole. Přejděte k dalšímu kroku.

Krok 4. Dokončení průvodce

Ukončete průvodce. Bude vytvořena nová zásada aplikace Kaspersky Endpoint Security.

Endpoint Detection and Response Agent (EDR Agent)

Počínaje Kaspersky Endpoint Security 12.3 pro systém Windows obsahuje aplikace konfiguraci Endpoint Detection and Response Agent (EDR Agent). *Endpoint Detection and Response Agent* je aplikace, která se instaluje na jednotlivé pracovní stanice a servery v IT infrastruktuře organizace za účelem podpory následujících řešení Detection and Response:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (od verze 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (od verze 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premise) (od verze 12.11)

EDR Agent nepřetržitě monitoruje procesy běžící na těchto počítačích, otevřená síťová připojení a upravované soubory. Součásti ochrany a kontroly aplikace nejsou pro aplikaci EDR Agent k dispozici.

EDR Agent je kompatibilní s aplikacemi EPP třetích stran. To vám umožní používat spolu s řešením Detection and Response od společnosti Kaspersky nástroje zabezpečení infrastruktury třetích stran.

Pro nasazení aplikace EDR Agent musí být v počítači nainstalována součást Network Agent a počítač musí být přidán do konzoly aplikace Kaspersky Security Center. Chcete-li povolit interakci aplikace EDR Agent s aplikací Kaspersky Security Center, musíte nainstalovat modul plug-in pro správu aplikace Kaspersky Endpoint Security pro systém Windows. Nastavení aplikace EDR Agent můžete zadat pomocí zásad skupiny. Chcete-li integrovat apliaci EDR Agent, musíte nakonfigurovat integraci v příslušných částech zásad.

Pro podporu fungování řešení Kaspersky Detection and Response by musí být v infrastruktuře nainstalovány následující aplikace Kaspersky:



Endpoint

- Network Agent
- EDR Agent



Kaspersky Security Center

Modul plug-in administrace produktu Kaspersky Endpoint Security pro systém Windows



Řešení Detection and Response: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premise)

Instalace aplikace EDR Agent

Kaspersky Endpoint Security v konfiguraci Endpoint Detection and Response Agent (EDR Agent) pro řešení Kaspersky Detection and Response se instaluje stejným způsobem.

Aplikaci EDR Agent lze do počítače nainstalovat jedním z následujících způsobů:

- Vzdáleně prostřednictvím aplikace Kaspersky Security Center.
- Místně pomocí průvodce instalací.
- Místně na příkazovém řádku (pouze pro KATA (EDR) a EDR Expert (on-premise)).

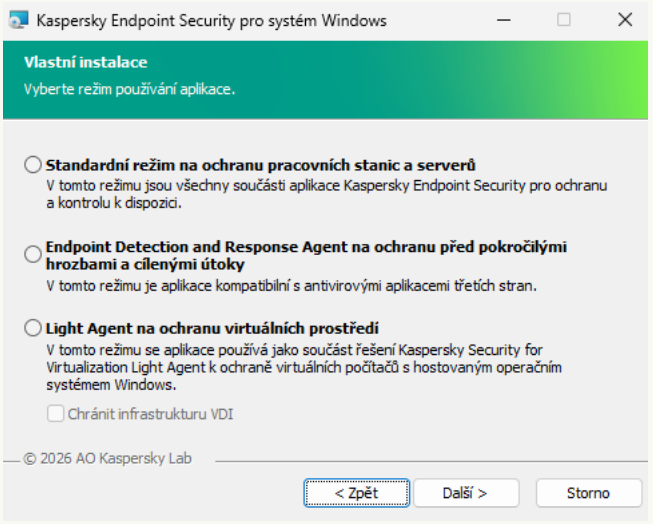
Chcete-li nainstalovat aplikaci EDR Agent, musíte vybrat vhodnou konfiguraci v nastavení instalačního balíčku nebo v průvodci instalací.

Jak nainstalovat aplikaci EDR Agent pomocí průvodce instalací

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

Spustí se Průvodce instalací.

Konfigurace aplikace Kaspersky Endpoint Security



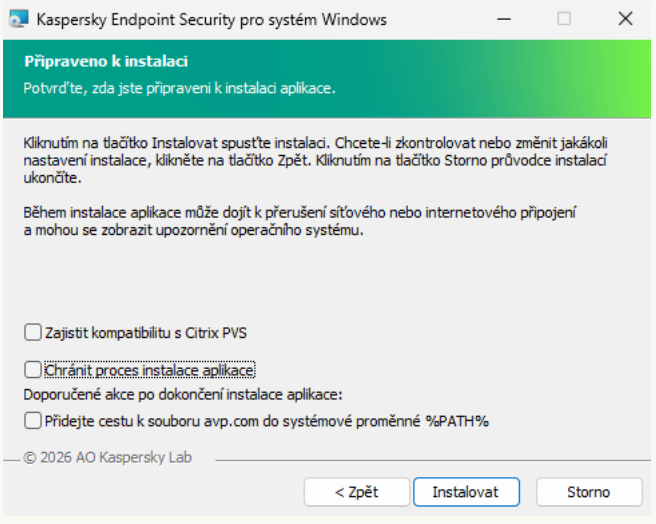
Výběr konfigurace aplikace

Vyberte konfiguraci **Endpoint Detection and Response Agent**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

Součásti aplikace Kaspersky Endpoint Security

Vyberte součásti, který chcete nainstalovat. Dostupné součásti aplikace můžete změnit po instalaci aplikace. Chcete-li tak učinit, musíte znovu spustit průvodce instalací 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 Windows Remote Desktop), doporučujeme ochranu instalace vypnout.

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

Přidejte cestu k souboru avp.com do systémové proměnné %PATH%. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku.

Jak nainstalovat aplikaci EDR Agent na příkazovém řádku (pouze pro KATA (EDR) a EDR Expert (on-premise))

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 /pSTANDALONEMODE=1 [/s]

   nebo

   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]

Jako výsledek je v počítači nainstalována aplikace EDR Agent pro integraci s platformou Kaspersky Anti Targeted Attack Platform (EDR) nebo Kaspersky Endpoint Detection and Response Expert (on-premise). Potvrdit, zda je aplikace nainstalována, a zkontrolovat nastavení aplikace, můžete vydáním příkazu `status`.

Jak nainstalovat EDR Agent pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole vyberte možnosti **Advanced** → **Remote installation** → složku **Installation packages**.

   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.
3. Otevřete vlastnosti instalačního balíčku.

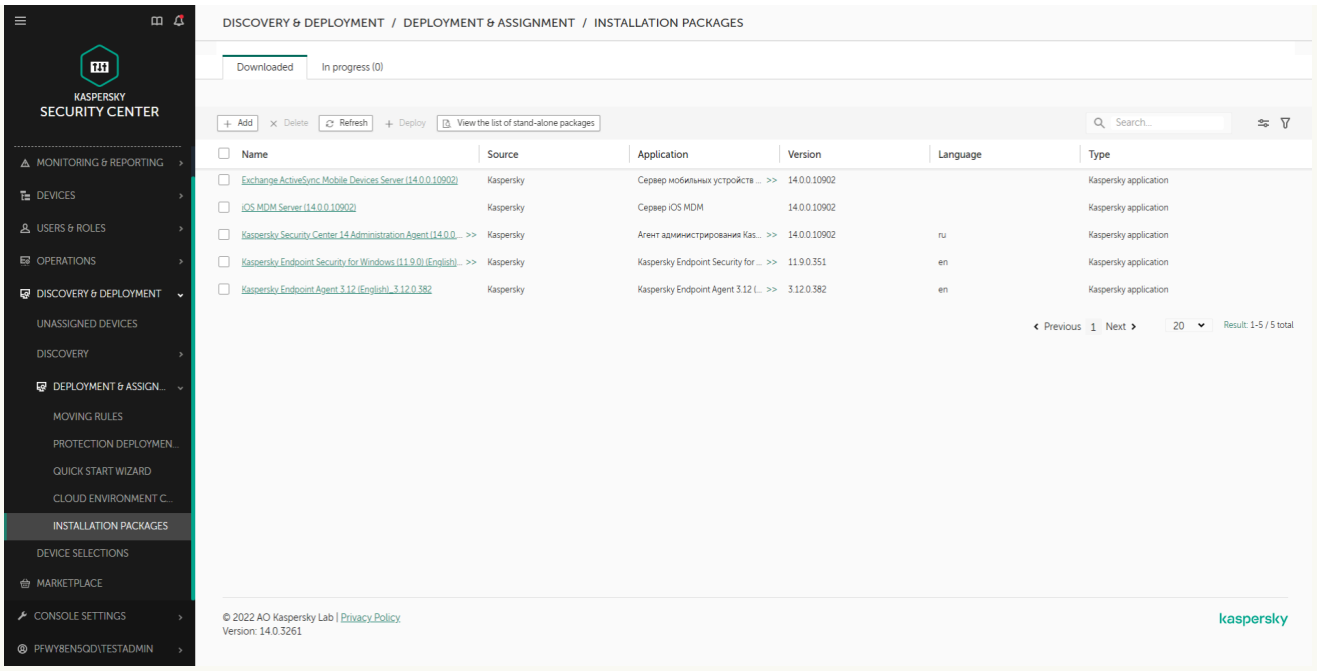
   Pokud je potřeba, vytvořte nový instalační balíček.
4. Přejděte do části **Protection components**.
5. Vyberte konfiguraci **Endpoint Detection and Response Agent na ochranu před pokročilými hrozbami a cílenými útoky**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.
6. Vyberte součásti, který chcete nainstalovat.

   Dostupné součásti aplikace můžete změnit po instalaci aplikace.
7. Uložte změny.
8. Vytvořte úlohu vzdálené instalace. Ve vlastnostech úlohy vyberte instalační balíček, který jste vytvořili.

Jak nainstalovat aplikaci EDR Agent pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

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



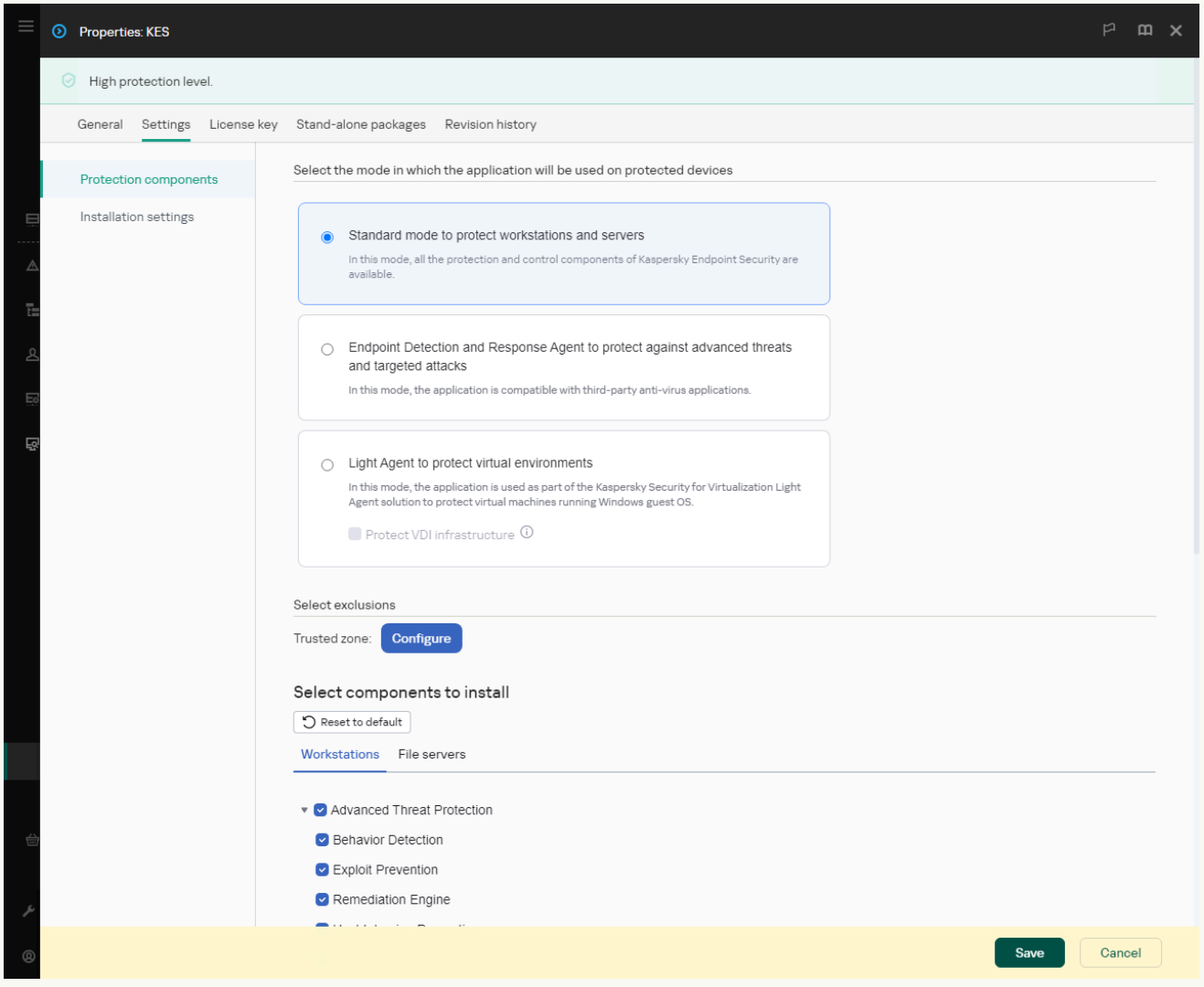
Seznam instalačních balíčků

2. Otevřete vlastnosti instalačního balíčku.

   Pokud je potřeba, vytvořte nový instalační balíček.

3. Vyberte kartu **Settings**.

4. Přejděte do části **Protection components**.



Součásti obsažené v instalačním balíčku

5. Vyberte konfiguraci **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. V této konfiguraci můžete nainstalovat pouze součásti, které poskytují podporu pro řešení Detection and Response: MDR, EDR (KATA), NDR (KATA), Expert na EDR (on-premise) a KUMA. Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením Kaspersky Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

6. Vyberte součásti, který chcete nainstalovat.

   Dostupné součásti aplikace můžete změnit po instalaci aplikace.

7. Uložte změny.

8. Vytvořte úlohu vzdálené instalace. Ve vlastnostech úlohy vyberte instalační balíček, který jste vytvořili.

Aplikace EDR Agent je nainstalována v počítači uživatele. Můžete použít rozhraní aplikace a v oznamovací oblasti se zobrazí ikona aplikace.

V aplikaci Kaspersky Security Center má počítač s nainstalovanou aplikací v konfiguraci EDR Agent stav *Critical* – . Počítač má tento stav, protože chybí součást Ochrana před souborovými hrozbami. Nemusíte podnikat žádné další kroky.

Pokud se vám nepodařilo nainstalovat aplikaci EDR Agent do počítače s aplikací EPP třetí strany, protože instalační program našel v počítači nekompatibilní software, můžete přeskočit kontrolu nekompatibilního softwaru.



Hlavní okno aplikace EDR Agent

Nyní musíte nakonfigurovat integraci s řešením Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) nebo Kaspersky Anti Targeted Attack (NDR). Můžete také určit rozšířená nastavení aplikace a např. vytvořit důvěryhodnou zónu nebo skrýt rozhraní aplikace. K dispozici jsou nastavení v následujících sekcích:

- Kaspersky Security Network
- Nastavení aplikace
- Nastavení sítě
- Výjimky

- Zprávy
- Rozhraní
- Správa nastavení

Integrace aplikace EDR Agent s MDR

Aplikace EDR Agent se instaluje na pracovních stanicích a serverech v IT infrastruktuře organizace. EDR Agent zpracovává data a odesílá je prostřednictvím streamů Kaspersky Security Network do řešení Kaspersky Managed Detection and Response.

Aby součást Kaspersky Managed Detection and Response fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*. Kaspersky Managed Detection and Response vás vyzve k navázání připojení na pozadí, když nasazujete toto řešení. Ujistěte se, že je připojení na pozadí navázáno.

Navázání připojení na pozadí ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Settings** → **Integration**.
2. Přejděte do části **Integration**.
3. Zapněte přepínač **Background connection for integration Enabled**.
4. Uložte změny.

Integrace s řešením Kaspersky Managed Detection and Response sestává z následujících kroků:

1. **Instalace součásti Managed Detection and Response**

   Součást MDR můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

   Pro dokončení aktualizace aplikace novými součástmi je nutné restartovat počítač.

2. **Kaspersky Private Security Network**

   Pokud používáte cloudovou konzolu aplikace Kaspersky Security Center, tento krok přeskočte. Cloudová konzola aplikace Kaspersky Security Center automaticky konfiguruje Kaspersky Private Security Network při instalaci modulu plug-in MDR.

   Kaspersky Private Security Network (KPSN) 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.

   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. Podrobnosti o konfiguraci služby Kaspersky Private Security Network najdete v nápovědě k aplikaci Kaspersky Security Center. Konfigurační soubor služby Kaspersky Security Network můžete také nahrát do počítače z příkazového řádku (viz pokyny níže).

   Jak nakonfigurovat službu Kaspersky Private Security Network 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. Spusťte následující příkaz:

      avp.com KSN /private <file name>

      kde `<file name>` je název konfiguračního souboru obsahujícího nastavení služby Kaspersky Private Security Network (formát souboru PKCS7 nebo PEM).

      Příklad:

      ```
      avp.com KSN /private C:\kpsn_config.pkcs7
      ```

   Aplikace Kaspersky Endpoint Security tak bude používat službu Kaspersky Private Security Network k určení reputace souborů, aplikací a webů. V části s nastavením zásad **Kaspersky Security Network** se zobrazí následující provozní stav: *Infrastruktura: Kaspersky Private Security Network*.

Aby mohla součást Managed Detection and Response fungovat, musíte povolit rozšířený režim KSN.

3 **Aktivace řešení Kaspersky Managed Detection and Response**

Počínaje aplikací Kaspersky Endpoint Security pro systém Windows 12.10 můžete pro aktivací funkce Managed Detection and Response jako alternativu k aktivačnímu kódu používat také soubor klíče.

Musíte si koupit samostatnou licenci pro MDR (doplněk součásti Kaspersky Managed Detection and Response).

Funkce bude k dispozici poté, co pro doplněk Kaspersky Managed Detection and Response zadáte samostatný klíč. Fungování licence k samostatné funkci Managed Detection and Response je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

Ověřte, zda je funkce MDR součástí licence a je spuštěna v místním rozhraní aplikace.

4 **Povolení součásti Managed Detection and 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 nápovědě k řešení Kaspersky Managed Detection and Response.

Počínaje Kaspersky Endpoint Security 12.6 pro systém Windows je přidání souboru BLOB volitelné pro Kaspersky Managed Detection and Response bez tenantů, pokud máte aktuální licenci.

Jak povolit součást Managed Detection and Response v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaškrtněte políčko **Managed Detection and Response (Industrial CyberSecurity)**.
5. V bloku **Nastavení** klikněte na možnost **Nahrát** a vyberte soubor BLOB obdržený v konzole aplikace Kaspersky Managed Detection and Response. Soubor má příponu P7.

   Ve výchozím nastavení může uživatel spravovat nastavení aplikace („visací zámek" je otevřený). Chcete-li zásady použít v počítačích, zavřete zámky.
6. Uložte změny.

Jak povolit součást Managed Detection and Response ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration → Managed Detection and Response**.
5. Zapněte přepínač **Managed Detection and Response ENABLED**.
6. Klikněte na tlačítko **Upload** a vyberte soubor BLOB, který byl získán v konzole řešení Managed Detection and Response. Soubor má příponu P7.

   Ve výchozím nastavení může uživatel spravovat nastavení zásad („visací zámek" je otevřený). Chcete-li zásady použít v počítačích, zavřete zámky.
7. Uložte změny.

Jak povolit součást Managed Detection and Response 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. Spusťte následující příkaz:

   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>

   Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Konfigurace nastavení aplikace**.

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 stáhne a odešle jej do počítače během další synchronizace s aplikací Kaspersky Security Center. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. 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.

5 **Konfigurace jiných součástí aplikace pro příjem telemetrie**

Aby mohla součást Managed Detection and Response fungovat, musíte povolit následující součásti:

- Kaspersky Security Network (rozšířený režim).
- Detekce chování.
- Prevence zneužití.
- Ochrana před webovými hrozbami.
- Ochrana před hrozbami v poště.
- Ochrana před souborovými hrozbami.
- Ochrana před síťovými hrozbami.
- Brána firewall.
- Ochrana AMSI.
- Kontrola na pozadí.

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Zapněte přepínač **Managed Detection and Response ENABLED**.
6. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaškrtněte políčko **Managed Detection and Response (Industrial CyberSecurity)**.
5. Uložte změny.

Integrace aplikace EDR Agent s EDR (KATA)

Aplikace EDR Agent se instaluje na pracovních stanicích a serverech v IT infrastruktuře organizace. Na těchto počítačích EDR Agent nepřetržitě monitoruje procesy, otevřená síťová připojení a upravované soubory a odesílá údaje z monitorování na server se součástí Central Node.

Chcete-li provést integraci s EDR (KATA), musíte povolit součást Endpoint Detection and Response (KATA) a nakonfigurovat agenta EDR Agent.

Aby součást Endpoint Detection and Response (KATA) fungovala, musí být splněny tyto podmínky:

- Kaspersky Anti Targeted Attack Platform verze 5.0–7.1.
- Kaspersky Security Center verze 14.2 nebo novější. Ve starších verzích aplikace Kaspersky Security Center není možné funkci Endpoint Detection and Response (KATA) aktivovat.

Integrace s řešením Endpoint Detection and Response (KATA) sestává z následujících kroků:

1. **Aktivace součásti Endpoint Detection and Response (KATA)**

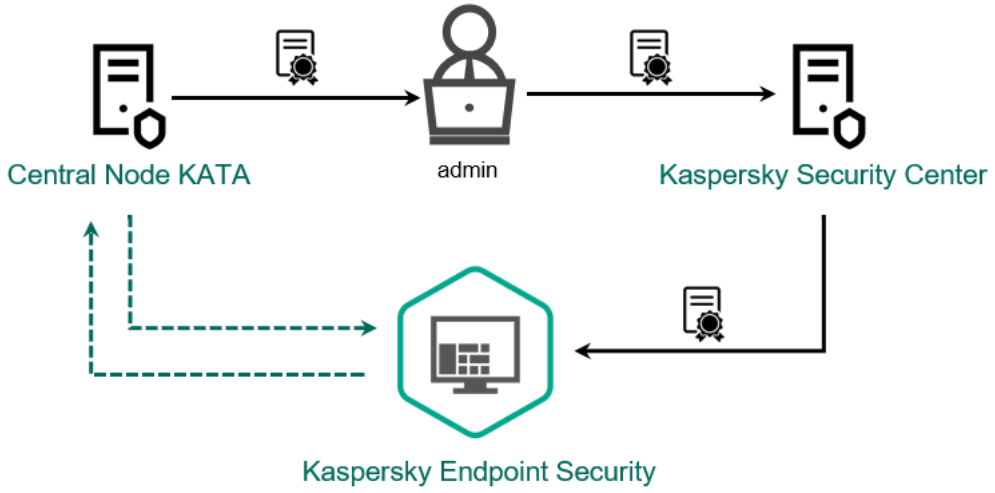
   Musíte si koupit samostatnou licenci pro EDR (KATA) (doplněk součásti Kaspersky Endpoint Detection and Response (KATA)).

   Funkce bude k dispozici poté, co pro Kaspersky Endpoint Detection and Response (KATA) zadáte samostatný klíč. Fungování licence k samostatné funkci Endpoint Detection and Response (KATA) je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

   Ověřte, zda je funkce EDR (KATA) součástí licence a je spuštěna v místním rozhraní aplikace.

2. **Připojení k součásti Central Node**

   Součást Kaspersky Anti Targeted Attack Platform vyžaduje vytvoření důvěryhodného spojení mezi aplikací Kaspersky Endpoint Security a součástí Central Node. Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).



Přidání certifikátu TLS do aplikace Kaspersky Endpoint Security

   Ve výchozím nastavení Kaspersky Endpoint Security kontroluje pouze certifikát TLS součásti Central Node. Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače na součásti Central Node (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení součásti Central Node a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Detection and Response → Endpoint Detection and Response Expert (on-premise)**.
5. Zaškrtněte políčko **Endpoint Detection and Response Expert (on-premise)**.
6. Klikněte na tlačítko **Nastavení připojení k serveru**.
7. Nakonfigurujte připojení k serveru:
   - **Doba vypršení časového limitu (s)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Certifikát TLS serveru**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
   - **Používat ověřování na obou stranách**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.
8. Klikněte na tlačítko **OK**.
9. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

   Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
10. V případě potřeby nakonfigurujte telemetrii.
11. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte kartu **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premise)**.
5. Zapněte přepínač **Endpoint Detection and Response Expert (on-premise) ENABLED**.
6. Chcete-li nakonfigurovat EDR (KATA), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
7. Klikněte na tlačítko **Connection settings**.
8. Nakonfigurujte připojení k serveru:
   - **Timeout (sec)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).

- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

  Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

9. Klikněte na tlačítko **OK**.
10. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

    Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
11. V případě potřeby nakonfigurujte telemetrii.
12. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Počítač je tak přidán do konzoly součásti Kaspersky Anti Targeted Attack Platform. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Endpoint Detection and Response Expert (on-premise)** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Integrace aplikace EDR Agent s NDR (KATA)

Aplikace EDR Agent se instaluje na pracovních stanicích a serverech v IT infrastruktuře organizace. Na těchto počítačích EDR Agent nepřetržitě monitoruje procesy, otevřená síťová připojení a upravované soubory a odesílá údaje z monitorování na server se součástí Central Node.

Chcete-li provést integraci s NDR (KATA), musíte povolit součást Network Detection and Response (KATA) a nakonfigurovat agenta EDR Agent.

Aby součást Network Detection and Response (KATA) fungovala, musí být splněny tyto podmínky:

- Kaspersky Anti Targeted Attack Platform verze 7.0 nebo novější.
- Kaspersky Security Center verze 14.2 nebo novější. Ve starších verzích aplikace Kaspersky Security Center není možné funkci Network Detection and Response (KATA) aktivovat.

Integrace s řešením Network Detection and Response (KATA) sestává z následujících kroků:

1. **Aktivace součásti Network Detection and Response (KATA)**

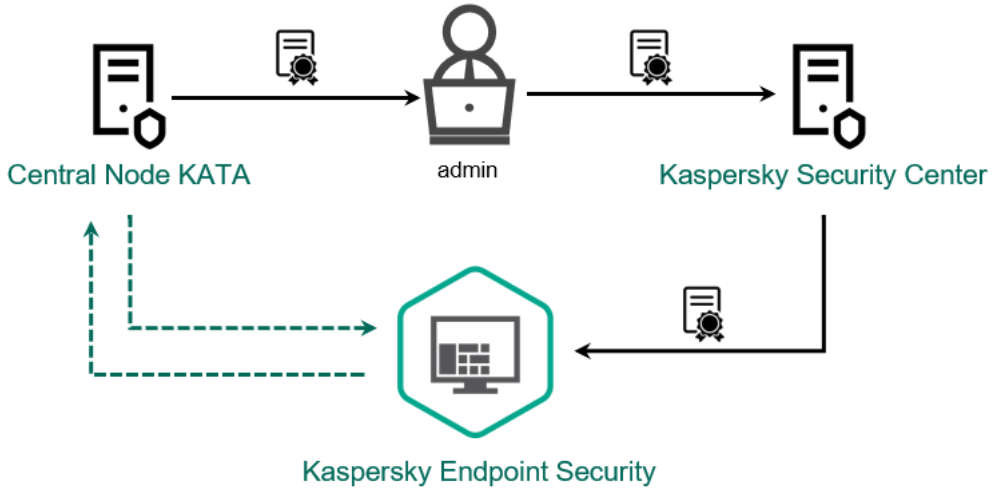
   Musíte si koupit samostatnou licenci pro NDR (KATA) (doplněk součásti Kaspersky Network Detection and Response (KATA)).

   Funkce bude k dispozici poté, co pro Kaspersky Network Detection and Response (KATA) zadáte samostatný klíč. Fungování licence k samostatné funkci Network Detection and Response (KATA) je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

   Ověřte, zda je funkce NDR (KATA) součástí licence a je spuštěna v místním rozhraní aplikace.

2. **Připojení k součásti Central Node**

Součást Kaspersky Anti Targeted Attack Platform vyžaduje vytvoření důvěryhodného spojení mezi aplikací Kaspersky Endpoint Security a součástí Central Node. Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).



Přidání certifikátu TLS do aplikace Kaspersky Endpoint Security

Ve výchozím nastavení Kaspersky Endpoint Security kontroluje pouze certifikát TLS součásti Central Node. Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače na součásti Central Node (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení součásti Central Node a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Detection and Response** → **Network Detection and Response (KATA)**.
4. Zaškrtněte políčko **Network Detection and Response (KATA)**.
5. Klikněte na tlačítko **Connection settings**.
6. Nakonfigurujte připojení k serveru:
   - **Timeout (sec)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.
7. Klikněte na tlačítko **OK**.
8. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.
9. Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
10. V případě potřeby nakonfigurujte telemetrii.
11. Uložte změny.

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.
5. Zapněte přepínač **Network Detection and Response (KATA) ENABLED**.
6. Klikněte na tlačítko **Connection settings**.
7. Nakonfigurujte připojení k serveru:
   - **Timeout (sec)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.
8. Klikněte na tlačítko **OK**.
9. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.
10. Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
11. V případě potřeby nakonfigurujte telemetrii.
12. Uložte změny.

Počítač je tak přidán do konzoly součásti Kaspersky Anti Targeted Attack Platform. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Network Detection and Response (KATA)** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Integrace aplikace EDR Agent s EDR Expert (on-premise)

Aplikace EDR Agent se instaluje na pracovních stanicích a serverech v IT infrastruktuře organizace. Na těchto počítačích EDR Agent nepřetržitě monitoruje procesy, otevřená síťová připojení a upravované soubory a odesílá údaje z monitorování na server EDR Expert (on-premise).

Chcete-li provést integraci s řešením EDR Expert (on-premise), musíte povolit součást Endpoint Detection and Response Expert (on-premise) a nakonfigurovat agenta EDR Agent.

Integrace s řešením Endpoint Detection and Response Expert (on-premise) sestává z následujících kroků:

1. **Aktivace součásti Kaspersky Endpoint Detection and Response Expert (on-premise)**

   Musíte si koupit samostatnou licenci pro EDR Expert (on-premise) (doplněk součásti Kaspersky Endpoint Detection and Response Expert (on-premise)).

   Funkce bude k dispozici poté, co pro Kaspersky Endpoint Detection and Response Expert (on-premise) zadáte samostatný klíč. Fungování licence k samostatné funkci Endpoint Detection and Response Expert (on-premise) je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

   Ověřte, zda je funkce EDR Expert (on-premise) součástí licence a je spuštěna v místním rozhraní aplikace.
2. **Připojování k serveru pro shromažďování telemetrie a odpovědní server**

Kaspersky Endpoint Detection and Response Expert (on-premise) vyžaduje důvěryhodné připojení mezi aplikací Kaspersky Endpoint Security a dvěma servery:

- *Server pro shromažďování telemetrie* je server, který je součástí řešení SIEM, které shromažďuje, normalizuje, uvádí do vzájemného vztahu, analyzuje a ukládá informace o událostech, k nimž dochází v počítači.
- *Odpovědní server* je server pro příjem a kontrolu dat, studium chování objektů a publikování výsledků těchto studií.

Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).

Ve výchozím nastavení Kaspersky Endpoint Security kontroluje pouze certifikát TLS serverů. Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače na serveru (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení serveru a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).

Jak připojit počítač Kaspersky Endpoint Security k součásti EDR Expert (on-premise) pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premise)**.
5. Zapněte přepínač **Endpoint Detection and Response Expert (on-premise) ENABLED**.
6. Chcete-li nakonfigurovat EDR Expert (on-premise), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 8.0 or later)**.
7. Nakonfigurujte připojení k *serverům pro shromažďování telemetrie*:
   a. V bloku **Connection to telemetry collection servers** klikněte na odkaz **Connection settings**.
   b. Nakonfigurujte připojení k serverům pro shromažďování telemetrie:
      - **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru.
      - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).
      - **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

        Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

   c. Klikněte na tlačítko **OK**.
   d. Přidejte servery pro shromažďování telemetrie. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

      Můžete přidat více adres serveru pro shromažďování telemetrie. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
   e. V případě potřeby nakonfigurujte telemetrii.
8. Nakonfigurujte připojení k *odpovědním serverům*:
   a. V bloku **Connection to response servers** nakonfigurujte nastavení **Send sync request to server every (min)**. Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace aplikace Kaspersky Endpoint Security přijímá úlohy reakce na hrozby a odesílá jejich výsledky.

b. Klikněte na odkaz **Connection settings**.

c. Nakonfigurujte připojení k odpovědním serverům:

- **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru.
- **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).
- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

  Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

d. Klikněte na tlačítko **OK**.

e. Přidejte odpovědní servery. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

Můžete přidat více adres odpovědních serverů. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.

9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Počítač je tak přidán do platformy OSMP (Open Single Management Platform). Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Endpoint Detection and Response Expert (on-premise)** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Kompatibilita s aplikacemi EPP třetích stran

EDR Agent podporuje funkce řešení Kaspersky Detection and Response. Součásti ochrany a kontroly nejsou pro aplikaci EDR Agent k dispozici. Tato konfigurace umožňuje instalaci aplikací EPP třetích stran a nasazení řešení Kaspersky Detection and Response v infrastruktuře organizace. EDR Agent podporuje práci s řešeními Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack Platform (EDR) a Kaspersky Anti Targeted Attack Platform (NDR).

EDR Agent je kompatibilní s aplikacemi EPP od následujících dodavatelů:

- **Dr.Web**

  EDR Agent je kompatibilní s nástrojem Dr.Web Agent pro Windows verze 13.0.1 nebo novější a Dr. Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent je kompatibilní s Dallas Lock 8.0-C verze 11.4.2.843 nebo novější.

  Aby součást EDR Agent běžela v počítači, na kterém je nainstalován software Dallas Lock, musíte v nastavení modulu Brána firewall povolit připojení k externím službám Kaspersky.

- **Secret Net Studio**

  EDR Agent je kompatibilní s Secret Net Studio verze 8.11 nebo novější.

  Aplikaci nelze nainstalovat do počítače, kde je nasazen software Secret Net Studio se součástí Antivirus. Aby byla interoperabilita možná, musíte součást Antivirus ze softwaru Secret Net Studio odebrat.

- **Trend Micro**

  EDR Agent je kompatibilní s aplikací Trend Micro Apex One verze 14.0.12994 nebo novější (včetně Security Agent).

  EDR Agent je kompatibilní s aplikací Trend Micro Deep Security verze 20.0.2-4960 nebo novější (včetně Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent je kompatibilní s aplikací Sophos Intercept X verze 2024.1.2 nebo novější (včetně Endpoint Agent) a Sophos Core Agent verze 2024.3.2.3.

- **Bitdefender**

  EDR Agent je kompatibilní s Bitdefender Endpoint Security Tools verze 7.9.21.523 nebo novější.

- **ESET**

  EDR Agent je kompatibilní s aplikací ESET Endpoint Security verze 12.0.2049.0 nebo novější a ESET Management Agent verze 12.0 nebo novější.

V počítačích se systémem Windows 11 pro Arm64 není EDR Agent kompatibilní s Bitdefender Endpoint Security Tools.

Aplikace musí být nainstalovány v následujícím pořadí: nejprve nainstalujte aplikaci EPP, poté aplikaci Kaspersky Security Center Network Agent a poté aplikaci EDR Agent. To je nezbytné, protože instalační program aplikace EPP může detekovat aplikace EDR Agent a Network Agent jako nekompatibilní software a odebrat je. Činnost aplikace EDR Agent a Network Agent by měla být také zkontrolována po aktualizaci aplikace EPP třetí strany, protože její instalační program může znovu vyhledat nekompatibilní software v počítači a aplikace odebrat.

Pokud se vám nepodařilo nainstalovat aplikaci EDR Agent do počítače s aplikací EPP třetí strany, protože instalační program našel v počítači nekompatibilní software, můžete přeskočit kontrolu nekompatibilního softwaru.

Managed Detection and Response



Kaspersky Endpoint Security pro systém Windows podporuje integraci s řešením Managed Detection and Response. Řešení *Kaspersky Managed Detection and Response (MDR)* automaticky detekuje a analyzuje bezpečnostní incidenty ve vaší infrastruktuře. K tomu používá MDR telemetrická data přijatá z koncových bodů a strojové učení. MDR zasílá údaje o incidentech odborníkům společnosti Kaspersky. Tito odborníci pak mohou incident zpracovat a například přidat nový záznam do antivirových databází. Alternativně mohou odborníci vydat doporučení ke zpracování incidentu a například navrhnout izolaci počítače od sítě. Podrobné informace o tom, jak řešení funguje, najdete v nápovědě k aplikaci Kaspersky Managed Detection and Response.

Konfigurace aplikace Kaspersky Endpoint Security pro integraci s MDR

Pro práci s MDR lze použít následující konfigurace:

- **[KES+integrovaný agent]**. V této konfiguraci se aplikace Kaspersky Endpoint Security chová jako aplikace zajišťující zabezpečení počítače i jako aplikace pro fungování s MDR. Integrovaný agent je dostupný v aplikaci Kaspersky Endpoint Security 11.6.0 pro systém Windows nebo novější.

- **[EPP třetí strany+EDR Agent]**. V této konfiguraci je zabezpečení IT infrastruktury zajištěno platformou Endpoint Protection Platform (EPP) třetí strany. Interakci s MDR zajišťuje Kaspersky Endpoint Security v konfiguraci Endpoint Detection and Response Agent (EDR Agent). V této konfiguraci je EDR Agent kompatibilní s aplikacemi EPP třetích stran. EDR Agent je k dispozici v aplikaci Kaspersky Endpoint Security 12.3 pro systém Windows nebo novější.

Podpora pro předchozí verze Kaspersky Endpoint Security

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 MDR aktualizovat databáze na nejnovější verzi. Musíte rovněž nainstalovat aplikaci Kaspersky Endpoint Agent.

Pokud používáte Kaspersky Endpoint Security 11.6.0 nebo novější a chcete používat Kaspersky Endpoint Agent, nemusíte instalovat řešení MDR.

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.

Integrace integrovaného agenta s MDR

Chcete-li nastavit integraci s řešením Kaspersky Managed Detection and Response Optimum, musíte povolit součást Managed Detection and Response a nakonfigurovat aplikaci Kaspersky Endpoint Security.

Aby součást Kaspersky Managed Detection and Response fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*. Kaspersky Managed Detection and Response vás vyzve k navázání připojení na pozadí, když nasazujete toto řešení. Ujistěte se, že je připojení na pozadí navázáno.

Navázání připojení na pozadí ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Settings** → **Integration**.
2. Přejděte do části **Integration**.
3. Zapněte přepínač **Background connection for integration Enabled**.
4. Uložte změny.

Integrace s řešením Kaspersky Managed Detection and Response sestává z následujících kroků:

1 **Instalace součásti Managed Detection and Response**

Součást MDR můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

Pro dokončení aktualizace aplikace novými součástmi je nutné restartovat počítač.

2 **Kaspersky Private Security Network**

Pokud používáte cloudovou konzolu aplikace Kaspersky Security Center, tento krok přeskočte. Cloudová konzola aplikace Kaspersky Security Center automaticky konfiguruje Kaspersky Private Security Network při instalaci modulu plug-in MDR.

Kaspersky Private Security Network (KPSN) 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.

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. Podrobnosti o konfiguraci služby Kaspersky Private Security Network najdete v nápovědě k aplikaci Kaspersky Security Center. Konfigurační soubor služby Kaspersky Security Network můžete také nahrát do počítače z příkazového řádku (viz pokyny níže).

Jak nakonfigurovat službu Kaspersky Private Security Network 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. Spusťte následující příkaz:

   avp.com KSN /private <file name>

   kde `<file name>` je název konfiguračního souboru obsahujícího nastavení služby Kaspersky Private Security Network (formát souboru PKCS7 nebo PEM).

   Příklad:

   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Aplikace Kaspersky Endpoint Security tak bude používat službu Kaspersky Private Security Network k určení reputace souborů, aplikací a webů. V části s nastavením zásad **Kaspersky Security Network** se zobrazí následující provozní stav: *Infrastruktura: Kaspersky Private Security Network.*

Aby mohla součást Managed Detection and Response fungovat, musíte povolit rozšířený režim KSN.

3 **Aktivace řešení Kaspersky Managed Detection and Response**

Počínaje aplikací Kaspersky Endpoint Security pro systém Windows 12.10 můžete pro aktivací funkce Managed Detection and Response jako alternativu k aktivačnímu kódu používat také soubor klíče.

Kaspersky Managed Detection and Response podporuje následující metody licencování:

- Funkce Managed Detection and Response je součástí licence k aplikaci Kaspersky Endpoint Security pro systém Windows.

  Tato funkce je k dispozici okamžitě po aktivaci aplikace Kaspersky Endpoint Security pro systém Windows.

- Používá se samostatná licence pro MDR (doplněk Kaspersky Managed Detection and Response).

  Funkce bude k dispozici poté, co pro doplněk Kaspersky Managed Detection and Response zadáte samostatný klíč. V počítači tak jsou přidány dva klíče: klíč pro aplikaci Kaspersky Endpoint Security a klíč pro řešení Kaspersky Managed Detection and Response.

  Fungování licence k samostatné funkci Managed Detection and Response je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

Ověřte, zda je funkce MDR součástí licence a je spuštěna v místním rozhraní aplikace.

4. **Povolení součásti Managed Detection and 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 nápovědě k řešení Kaspersky Managed Detection and Response.

Počínaje Kaspersky Endpoint Security 12.6 pro systém Windows je přidání souboru BLOB volitelné pro Kaspersky Managed Detection and Response bez tenantů, pokud máte aktuální licenci.

Jak povolit součást Managed Detection and Response v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaškrtněte políčko **Managed Detection and Response (Industrial CyberSecurity)**.
5. V bloku **Nastavení** klikněte na možnost **Nahrát** a vyberte soubor BLOB obdržený v konzole aplikace Kaspersky Managed Detection and Response. Soubor má příponu P7.

   Ve výchozím nastavení může uživatel spravovat nastavení aplikace („visací zámek" je otevřený). Chcete-li zásady použít v počítačích, zavřete zámky.
6. Uložte změny.

Jak povolit součást Managed Detection and Response ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration → Managed Detection and Response**.
5. Zapněte přepínač **Managed Detection and Response ENABLED**.
6. Klikněte na tlačítko **Upload** a vyberte soubor BLOB, který byl získán v konzole řešení Managed Detection and Response. Soubor má příponu P7.

   Ve výchozím nastavení může uživatel spravovat nastavení zásad („visací zámek" je otevřený). Chcete-li zásady použít v počítačích, zavřete zámky.
7. Uložte změny.

Jak povolit součást Managed Detection and Response 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. Spusťte následující příkaz:

avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Konfigurace nastavení aplikace**.

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 stáhne a odešle jej do počítače během další synchronizace s aplikací Kaspersky Security Center. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. 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.

5 **Konfigurace jiných součástí aplikace pro příjem telemetrie**

Aby mohla součást Managed Detection and Response fungovat, musíte povolit následující součásti:

- Kaspersky Security Network (rozšířený režim).
- Detekce chování.
- Prevence zneužití.
- Ochrana před webovými hrozbami.
- Ochrana před hrozbami v poště.
- Ochrana před souborovými hrozbami.
- Ochrana před síťovými hrozbami.
- Brána firewall.
- Ochrana AMSI.
- Kontrola na pozadí.

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Managed Detection and Response**.
5. Zapněte přepínač **Managed Detection and Response ENABLED**.
6. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**.
4. Zaškrtněte políčko **Managed Detection and Response (Industrial CyberSecurity)**.
5. Uložte změny.

Průvodce migrací KEA na KES pro MDR

Aplikace Kaspersky Endpoint Security pro systém Windows integrovaného agenta pro řešení Kaspersky Managed Detection and Response. Pro práci s řešením MDR už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent. Všechny funkce aplikace Kaspersky Endpoint Agent bude provádět aplikace Kaspersky Endpoint Security.

Když nasadíte Kaspersky Endpoint Security do počítačů s nainstalovanou aplikací Kaspersky Endpoint Agent, řešení Kaspersky Managed Detection and Response bude nadále fungovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent. Ke stejnému chování v systému dojde, když aktualizujete Kaspersky Endpoint Security na verzi 11.6.0 nebo novější.

Aplikace Kaspersky Endpoint Security není kompatibilní s aplikací Kaspersky Endpoint Agent. Obě tyto aplikace nelze nainstalovat do stejného počítače.

Aby aplikace Kaspersky Endpoint Security fungovala jako součást řešení Kaspersky Managed Detection and Response, musí být splněny následující podmínky:

- Kaspersky Security Center verze 13.2 nebo vyšší (včetně součásti Network Agent). Ve starších verzích aplikace Kaspersky Security Center není možné funkci Managed Detection and Response aktivovat.
- Je navázáno připojení na pozadí mezi webovou konzolou aplikace Kaspersky Security Center a serverem pro správu. Aby součást MDR fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*.

Kroky pro migraci konfigurace [KES+KEA] na [KES+integrovaný agent] pro MDR

1. **Upgrade modulu plug-in pro správu aplikace Kaspersky Endpoint Security**

   Součást MDR lze spravovat pomocí modulu plug-in pro správu aplikace Kaspersky Endpoint Security verze 11.6 nebo novější. V závislosti na typu konzoly aplikace Kaspersky Security Center, kterou používáte, aktualizujte modul plug-in pro správu v konzole pro správu (MMC) nebo webový modul plug-in ve webové konzole.

2. **Migrace zásady a úloh**

   Nastavení aplikace Kaspersky Endpoint Agent můžete přenést do aplikace Kaspersky Endpoint Security pro Windows. K dispozici jsou následující možnosti:

   - Průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security. Průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security funguje pouze ve webové konzole.

     Jak migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security ve webové konzole

     V hlavním okně webové konzoly vyberte možnosti **Operations → Migration from Kaspersky Endpoint Agent**.

     Tím spustíte průvodce migrací zásad a úloh. Postupujte podle pokynů průvodce.

     Krok 1. Migrace zásad

     Průvodce migrací vytvoří novou zásadu, která sloučí nastavení zásad aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete sloučit se zásadami aplikace Kaspersky Endpoint Security. Kliknutím na zásadu aplikace Kaspersky Endpoint Agent vyberte zásadu aplikace Kaspersky Endpoint Security, s níž chcete sloučit nastavení. Zkontrolujte, zda jste vybrali správné zásady, a přejděte k dalšímu kroku.

     Krok 2. Migrace úloh

     Průvodce migrací nepodporuje úlohy MDR. Tento krok přeskočte.

     Krok 3. Dokončení průvodce

     Ukončete průvodce. Bude vytvořena nová zásada aplikace Kaspersky Endpoint Security. V zásadě se sloučí nastavení z aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Název zásady je *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Nová zásada má stav *Inactive*. Chcete-li pokračovat, změňte stav zásad aplikací Kaspersky Endpoint Agent a Kaspersky Endpoint Security na *Inactive* a aktivujte novou sloučenou zásadu.

   - Standardní průvodce hromadným převodem zásad a úloh. Průvodce hromadným převodem zásad a úloh je k dispozici pouze v konzole pro správu (MMC). Další podrobnosti o průvodci hromadným převodem zásad a úloh naleznete v nápovědě k aplikaci Kaspersky Security Center.

3. **Licence k funkci MDR**

   Chcete-li aktivovat Kaspersky Endpoint Security jako součást řešení Kaspersky Anti Targeted Attack Platform, potřebujete samostatnou licenci pro doplněk Kaspersky Managed Detection and Response. Klíč můžete přidat pomocí úlohy *Add key*. Do aplikace tak budou přidány dva klíče: *Kaspersky Endpoint Security* a *Kaspersky Managed Detection and Response*.

4. **Instalace/upgrade aplikace Kaspersky Endpoint Security**

   Pro migraci funkce MDR během instalace nebo upgradu aplikace se doporučuje použít úlohu vzdálené instalace. Při vytváření úlohy vzdálené instalace je třeba v nastavení instalačního balíčku vybrat součást MDR.

   Aplikaci můžete také upgradovat následujícími způsoby:

   - Pomocí aktualizační služby Kaspersky.

- Místně pomocí průvodce instalací.

Aplikace Kaspersky Endpoint Security podporuje automatický výběr součástí při upgradu aplikace na počítači, na němž je nainstalována aplikace Kaspersky Endpoint Agent. Automatický výběr součástí závisí na oprávněních uživatelského účtu, který aplikaci upgraduje.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru EXE nebo MSI pod systémovým účtem (SYSTEM), Kaspersky Endpoint Security získá přístup k aktuálním licencím řešení Kaspersky. Pokud je tedy v počítači nainstalována aplikace Kaspersky Endpoint Agent a aktivováno řešení MDR, instalační program aplikace Kaspersky Endpoint Security automaticky nakonfiguruje sadu součástí a vybere součást MDR. Tím se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent. Spuštění instalačního programu MSI pod systémovým účtem (SYSTEM) se obvykle provádí při upgradu prostřednictvím aktualizační služby Kaspersky nebo při nasazování instalačního balíčku prostřednictvím aplikace Kaspersky Security Center.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru MSI pod uživatelským účtem bez oprávnění, Kaspersky Endpoint Security nemá přístup k aktuálním licencím řešení Kaspersky. V tomto případě aplikace Kaspersky Endpoint Security automaticky vybere součásti na základě sady součástí aplikace Kaspersky Endpoint Agent. Poté se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent.

Kaspersky Endpoint Security podporuje upgrade bez restartování počítače. Režim upgradu aplikace můžete vybrat ve vlastnostech zásad.

5 **Kontrola chodu aplikace**

Pokud je po instalaci nebo upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

- Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
- Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*. Pokud je stav součásti *Není součástí licence*, ujistěte se, že jste aktivovali funkci integrovaného agenta.
- V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.

Endpoint Detection and Response



Aplikace Kaspersky Endpoint Security pro systém Windows obsahuje integrovaného agenta pro řešení Kaspersky Endpoint Detection and Response Optimum (dále také „EDR Optimum"). Počínaje verzí 11.8.0 obsahuje aplikace Kaspersky Endpoint Security pro systém Windows integrovaného agenta pro řešení Kaspersky Endpoint Detection and Response Expert (dále také „EDR Expert"). *Kaspersky Endpoint Detection and Response* je řada řešení pro ochranu podnikové IT infrastruktury před pokročilými kybernetickými hrozbami. Funkce řešení kombinuje automatickou detekci hrozeb se schopností reagovat na tyto hrozby a čelit tak pokročilým útokům včetně nových exploitů, ransomwaru, bezsouborových útoků a metod využívajících legitimní systémové nástroje. EDR Expert nabízí více funkcí sledování hrozeb a reakce na ně než EDR Optimum. Podrobnosti o těchto řešeních najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

Nástroje Threat Intelligence

Kaspersky Endpoint Detection and Response používá tyto nástroje po potlačování bezpečnostních hrozeb (Threat Intelligence):

- Integrace s portálem Kaspersky Threat Intelligence Portal, který obsahuje a zobrazuje informace o reputaci souborů a adres URL.
- Databáze Kaspersky Threats.
- Infrastruktura cloudových služeb Kaspersky Security Network (dále také jen „KSN"), která poskytuje přístup k informacím o souborech, webových stránkách a reputaci softwaru v reálném čase ze znalostní báze společnosti Kaspersky. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikací společnosti Kaspersky na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků.
- Technologie Cloud Sandbox, která vám umožňuje spouštět zjištěné soubory v izolovaném prostředí a kontrolovat jejich reputaci.

Princip fungování řešení

Kaspersky Endpoint Detection and Response kontroluje a analyzuje vývoj hrozeb a poskytuje *bezpečnostním pracovníkům* nebo *správci* informace o potenciálním útoku, které jsou nezbytné pro včasnou reakci. Kaspersky Endpoint Detection and Response zobrazí podrobnosti o výstraze v samostatném okně. *Upozornění* je událost v podnikové IT infrastruktuře, kterou aplikace identifikovala jako neobvyklou nebo podezřelou a která může představovat bezpečnostní hrozbu pro podnikovou IT infrastrukturu. *Podrobnosti o výsledcích detekce* je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

Podpora pro předchozí verze Kaspersky Endpoint Security

Pokud používáte Kaspersky Endpoint Security 11.2.0–11.6.0 pro interoperabilitu se součástí Kaspersky Endpoint Detection and Response Optimum, součástí aplikace je Kaspersky Endpoint Agent. Aplikaci Kaspersky Endpoint Agent můžete nainstalovat, i když už v počítači je Kaspersky Endpoint Security. V aplikaci Kaspersky Endpoint Security 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady Kaspersky Endpoint Security.

Řešení Kaspersky Endpoint Detection and Response Expert nepodporuje interoperabilitu s aplikací Kaspersky Endpoint Agent. Řešení Kaspersky Endpoint Detection and Response Expert používá aplikaci Kaspersky Endpoint Security s integrovaným agentem (verze 11.8.0 a novější).

Integrace integrovaného agenta s EDR Optimum / EDR Expert

Pro integraci s řešením Kaspersky Endpoint Detection and Response musíte přidat součást Endpoint Detection and Response Optimum (EDR Optimum), nebo součást Endpoint Detection and Response Expert (EDR Expert) a nakonfigurovat aplikaci Kaspersky Endpoint Security.

Součásti EDR Optimum, EDR Expert a EDR (KATA) nejsou vzájemně kompatibilní.

Aby součást Endpoint Detection and Response fungovala, musí být splněny tyto podmínky:

- Kaspersky Security Center verze 13.2 nebo novější. Ve starších verzích aplikace Kaspersky Security Center není možné funkci Endpoint Detection and Response aktivovat.
- Modul plug-in administrace řešení Kaspersky Endpoint Detection and Response.

  Počínaje verzí 12.6 aplikace Kaspersky Endpoint Security bylo zobrazení podrobností o výstrahách přesunuto z modulu plug-in administrace aplikace Kaspersky Endpoint Security do modulu plug-in administrace EDR. Modul plug-in pro správu EDR je jediný modul plug-in pro práci s agenty v operačních systémech Windows, Mac a Linux. Nově budete při práci s řešením EDR Optimum pro vytváření úloh reakce na hrozby a modul pro správu EDR pro zobrazení podrobností o výstrahách potřebovat modul plug-in administrace Kaspersky Endpoint Security.
- Součást EDR Optimum jako součást aplikace Kaspersky Endpoint Security podporuje interakci s řešením Kaspersky Endpoint Detection and Response Optimum 2.0. Interakce s aplikací Kaspersky Endpoint Detection and Response Optimum verze 1.0 není podporována.
- Součást EDR Optimum lze spravovat ve webové konzole aplikace Kaspersky Security Center a cloudové konzole aplikace Kaspersky Security Center.

  Součást EDR Expert lze spravovat pouze pomocí cloudové konzoly aplikace Kaspersky Security Center. Tuto funkci nemůžete spravovat pomocí konzoly pro správu (MMC).
- Je aktivována aplikace a na její funkčnost se vztahuje licence.
- Součást Endpoint Detection and Response je zapnutá.
- Součásti aplikace, na nichž Endpoint Detection and Response závisí, jsou povolené a funkční. Endpoint Detection and Response závisí na následujících součástech:
  - Ochrana před souborovými hrozbami.
  - Ochrana před webovými hrozbami.
  - Ochrana před hrozbami v poště.
  - Prevence zneužití.
  - Detekce chování.
  - Prevence narušení hostitele.
  - Modul pro nápravu.
  - Adaptivní kontrola anomálií.

Integrace s řešením Kaspersky Endpoint Detection and Response sestává z následujících kroků:

1. **Instalace součásti Endpoint Detection and Response**

   Součást EDR Optimum a EDR Expert můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

   Pro dokončení aktualizace aplikace novými součástmi je nutné restartovat počítač.

2. **Aktivace řešení Kaspersky Endpoint Detection and Response**

   Licenci k používání řešení Kaspersky Endpoint Detection and Response můžete získat těmito způsoby:

   - Funkce Endpoint Detection and Response je součástí licence k aplikaci Kaspersky Endpoint Security pro systém Windows.

Tato funkce je k dispozici okamžitě po aktivaci aplikace Kaspersky Endpoint Security pro systém Windows.

- Zakoupení samostatné licence pro EDR Optimum nebo EDR Expert (doplněk Kaspersky Endpoint Detection and Response).

  Funkce bude k dispozici poté, co pro Kaspersky Endpoint Detection and Response zadáte samostatný klíč. V počítači tak jsou přidány dva klíče: klíč pro aplikaci Kaspersky Endpoint Security a klíč pro řešení Kaspersky Endpoint Detection and Response.

  Fungování licence k samostatné funkci Endpoint Detection and Response je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

Ověřte, zda je funkce EDR Optimum součástí licence a je spuštěna v místním rozhraní aplikace.

Další informace o licenční smlouvě s koncovým uživatelem řešení EDR Optimum najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum.

3 Povolení součásti Endpoint Detection and Response

Součást můžete povolit nebo zakázat v nastavení zásad aplikace Kaspersky Endpoint Security pro systém Windows.

Jak povolit nebo zakázat součást Endpoint Detection and Response ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Zapněte přepínač **Endpoint Detection and Response ENABLED**.
6. Uložte změny.

Součást Kaspersky Endpoint Detection and Response je povolena. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Endpoint Detection and Response Optimum** nebo **Endpoint Detection and Response Expert** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

4 Povolení přenosu dat na server pro správu

Chcete-li aktivovat funkce součásti Endpoint Detection and Response, musí být povolen přenos pro následující typy dat:

- Data souborů v karanténě.

  Tato data jsou nutná k získání informací o souborech umístěných do karantény na počítači prostřednictvím webové konzoly a cloudové konzoly. Můžete si například stáhnout soubor z karantény za účelem analýzy ve webové konzole a cloudové konzole.

- Údaje o řetězci vývoje hrozeb.

  Tyto údaje jsou nutné k získání informací o hrozbách zjištěných na počítači ve webové konzole a cloudové konzole. Ve webové konzole a cloudové konzole můžete zobrazit podrobnosti o výstraze a provést akce v reakci na hrozbu.

Jak povolit přenos dat na server pro správu ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **KSC Integration**.
5. V bloku **Data transfer to Administration Server** klikněte na odkaz **Advanced settings**.
6. V okně, které se otevře, zaškrtněte následující políčka:
   - **About Quarantine files**.
   - **About a threat development chain**.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Vyhledávání indikátorů narušení (standardní úloha)

Indikátor narušení (IOC) je sada dat o objektu nebo činnosti, která indikuje neoprávněný přístup k počítači (narušení dat). Indikátor narušení může například představovat mnoho neúspěšných pokusů o přihlášení do systému. Úloha *IOC Scan* umožňuje v počítači najít tyto indikátory narušení a přijmout opatření jako reakci na hrozby.

Kaspersky Endpoint Security vyhledává indikátory narušení pomocí souborů IOC. *Soubory IOC* jsou soubory obsahující sady indikátorů, které se aplikace pokusí porovnat, aby započítala detekci. Soubory IOC musí odpovídat standardu OpenIOC.

Režim spuštění úlohy IOC Scan

Kaspersky Endpoint Detection and Response vám umožňuje vytvářet standardní úlohy kontroly IOC a zjišťovat tak data, u nichž došlo k narušení. *Standardní úloha kontroly IOC* je skupinová nebo místní úloha, která je vytvořena a nakonfigurována ručně ve webové konzole. Úlohy se spouštějí pomocí souborů IOC připravených uživatelem. Chcete-li přidat indikátor narušení ručně, přečtěte si požadavky na soubory IOC.

Soubor, který si můžete stáhnout kliknutím na níže uvedený odkaz, obsahuje tabulku s úplným seznamem podmínek IOC standardu OpenIOC.

STAŽENÍ SOUBORU IOC_TERMS.XLSX

Kaspersky Endpoint Security také podporuje samostatné úlohy kontroly IOC, když je aplikace používána jako součást řešení Kaspersky Sandbox.

Vytvoření souboru IOC

Počínaje aplikací Kaspersky Endpoint Security 12.10 pro systém Windows můžete soubory IOC vytvářet přímo v nastavení úlohy. Chcete-li vytvořit soubor IOC, musíte si připravit soubor TXT se seznamem indikátorů narušení. Jako indikátory narušení můžete přidat seznamy následujících objektů:

- Hodnoty hash souborů (MD5/SHA256).
  Aplikace připraví soubor IOC s rozsahem kontroly FileItem/Md5sum nebo FileItem/Sha256sum.
- IP adresy (IPv4, IPv6).
  Aplikace připraví soubor IOC s rozsahem kontroly PortItem/RemoteIP.
- Názvy DNS.
  Aplikace připraví soubor IOC s rozsahem kontroly DnsEntryItem/RecordName.

Jak vytvořit úlohu IOC ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Vyberte úlohu **IOC Scan**.
   Otevře se okno vlastností úlohy. V případě potřeby vytvořte úlohu **IOC Scan**.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **IOC Scan settings**.
5. Klikněte na tlačítko **Redefine IOC files**.
6. Otevře se formulář pro vytvoření souboru IOC:
   a. V části **IOC files source** vyberte možnost **Generate from file**.
   b. Zadejte název souboru IOC.
   c. Vyberte soubor TXT se seznamem indikátorů narušení.
   d. Vyberte typ souboru IOC: **DNS names**, **File hashes**, **IP addresses**.
   e. Klikněte na tlačítko **Generate**.

   Kaspersky Endpoint Security přidá soubory IOC do kolekce IOC. V případě potřeby můžete z rozsahu úlohy dočasně vyloučit soubory IOC.
7. Uložte změny.

Vytvoření úlohy IOC Scan

Úlohy *IOC Scan* můžete vytvářet ručně:

- V podrobnostech o výstraze (pouze EDR Optimum).

  Podrobnosti o výsledcích detekce je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

- Používání průvodce úlohami.

Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Postup vytvoření úlohy IOC Scan:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **IOC Scan**.

   c. Do pole **Task name** zadejte krátký popis.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Přejděte k dalšímu kroku.

5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Přejděte k dalšímu kroku.

   Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

   Systémový účet (SYSTEM) nemá oprávnění k provádění úloh *IOC Scan* na síťových jednotkách. Pokud chcete spustit úlohu pro síťovou jednotku, vyberte účet uživatele, který má k této jednotce přístup.

   U samostatných úloh Kontrola IOC u síťových jednotek musíte v nastavení úlohy ručně vybrat uživatelský účet, který má přístup k této jednotce.

6. Ukončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.

9. Přejděte do části **IOC Scan settings**.

10. Nahrajte soubory IOC a vyhledejte indikátory narušení.

    Po nahrání souborů IOC aplikace zobrazí souhrnné informace o souboru včetně seznamu indikátorů, které neprošly kontrolou. Po nahrání souborů IOC můžete soubory ručně upravit v integrovaném editoru přímo ve vlastnostech úlohy. Kaspersky Endpoint Security podporuje úpravy souborů IOC, které jsou v souladu se standardem OpenIOC 1.1. Obsah souborů IOC kompatibilních s OpenIOC verze 1.0 není možné upravovat.

    Kaspersky Endpoint Security přidá soubory IOC do kolekce IOC. V případě potřeby můžete z rozsahu úlohy dočasně vyloučit soubory IOC.

    Přidávání nebo odstraňování souborů IOC po spuštění úlohy se nedoporučuje. Může to způsobit nesprávné zobrazení výsledků kontroly IOC pro předchozí spuštění úlohy. Pro vyhledávání indikátorů narušení pomocí nových souborů IOC se doporučuje přidat nové úlohy.

11. V případě potřeby zaškrtněte políčko **Retrospective IOC Scan**. *Retrospektivní kontrola IOC* je režim úlohy *IOC Scan*, ve kterém aplikace Kaspersky Endpoint Security kontroluje indikátory narušení pomocí dat za určité časové období. Tento režim je určen pro hledání indikátorů narušení podle

telemetrie chráněného počítače, jako je síťová aktivita, procesy, soubory a jiná telemetrie. Kaspersky Endpoint Security analyzuje data v protokolech operačního systému a protokolech prohlížeče v počítači.

Retrospektivní kontrola IOC analyzuje protokoly následujících prohlížečů: Google Chrome, Mozilla Firefox, Microsoft Edge (verze 79 nebo novější).

12. Konfigurace akcí při detekci IOC:

- **Isolate device from the network**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security izoluje počítač od sítě, aby se zabránilo šíření hrozby. Dobu izolace můžete nakonfigurovat v nastavení součásti Endpoint Detection and Response.

  Není-li toto políčko zaškrtnuto, můžete po ručním spuštění úlohy izolovat počítač od sítě. Pokud úloha *IOC Scan* zjistí IOC, můžete počítač izolovat od sítě přímo z IOC (vlastnosti úlohy *IOC Scan* → **Application settings** → **IOC Scan results**). Aplikace Kaspersky Endpoint Security také umožňuje okamžitou správu dalších nastavení: Doba zakázání izolace od sítě a Výjimky z izolace od sítě.

- **Move copy to Quarantine, delete object**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security odstraní škodlivý objekt nalezený v počítači. Před odstraněním objektu vytvoří aplikace Kaspersky Endpoint Security záložní kopii pro případ, že bude nutné objekt později obnovit. Kaspersky Endpoint Security přesune záložní kopii do karantény.

  Není-li toto políčko zaškrtnuto, můžete soubor do karantény umístit ručně po ručním spuštění úlohy. Pokud úloha *IOC Scan* zjistí soubor, který může ohrozit data, můžete tento soubor umístit do karantény přímo ve výsledcích kontroly IOC (**Application settings** → **IOC Scan results**). Aplikace Kaspersky Endpoint Security tak spustí průvodce vytvořením úlohy s přednastavenými údaji o zjištěném souboru. Musíte pouze spravovat další nastavení úlohy, například nastavit plán úlohy.

- **Run Critical Areas Scan**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security spustí úlohu *Kontrola kritických oblastí*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků.

13. Přejděte do části **Advanced**.

14. Vyberte datové typy (dokumenty IOC), které je třeba analyzovat jako součást úlohy.

> Aplikace Kaspersky Endpoint Security automaticky vybírá datové typy (dokumenty IOC) pro úlohu *IOC Scan* v souladu s obsahem nahrávaných souborů IOC. Nedoporučujeme výběr datových typů rušit.

Kromě toho můžete nakonfigurovat rozsahy kontroly pro následující datové typy:

- **Files - FileItem**. Rozsah kontroly IOC v počítači nastavíte pomocí přednastavených rozsahů.

  Aplikace Kaspersky Endpoint Security standardně při kontrole vyhledává IOC pouze v důležitých oblastech počítače, jako je složka Stažené soubory, plocha, složka s dočasnými soubory operačního systému atd. Rozsah kontroly můžete také ručně přidat.

- **Windows event logs - EventLogItem**. Zadejte časové období, kdy byly události protokolovány. Můžete také vybrat, které protokoly událostí systému Windows mají být používány pro kontroly IOC. Ve výchozím nastavení jsou vybrány tyto protokoly událostí: protokol událostí aplikace, protokol událostí systému a protokol událostí zabezpečení.

- **Windows registry - RegistryItem**. Nakonfigurujte rozsah kontroly IOC v registru.

  Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje sadu klíčů registru.

15. V okně vlastností úlohy vyberte kartu **Schedule**.

16. Nakonfigurujte plán úloh.

> Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

17. Uložte změny.

18. Zaškrtněte políčko vedle úlohy.

19. Klikněte na tlačítko **Start**.

Aplikace Kaspersky Endpoint Security tak spustí v počítači hledání indikátorů narušení. Výsledky úlohy můžete zobrazit ve vlastnostech úlohy v části **Results**. Informace o zjištěných indikátorech narušení můžete zobrazit ve vlastnostech úlohy: **Application settings** → **IOC Scan results**. Ve výsledcích kontroly IOC můžete také ručně umístit zjištěný soubor do karantény nebo izolovat počítač od sítě.

Kaspersky Endpoint Security hledá duplikáty mezi záznamy vytvořenými pro stejný soubor IOC a ve výsledcích úloh uchovává pouze jedinečné záznamy. Duplikáty jsou záznamy stejného typu, které mají stejné hodnoty všech porovnávaných polí. Aplikace také nemusí vytvořit záznam, pokud mu chybí hodnota v jednom nebo více polích (viz tabulka níže).

Typ	Porovnávaná pole	Podmínka pro nevytvoření záznamu
FileItem	• FullPath • Md5sum • Sha256sum	• Chybí hodnota polí FullPath, Md5sum, Sha256sum. • Chybí hodnoty pole FullPath a shodují se hodnoty polí Md5sum, Sha256sum.

	• PID • UPID • ImagePath	
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	Chybí hodnota alespoň jednoho z následujících polí: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	Chybí hodnoty pole startTime nebo PID.

V okně **Alert Details** se mohou zobrazovat záznamy RegistryItem se shodnými hodnotami polí. Tyto záznamy nejsou duplicitní, protože mají různé hodnoty pole Text, které se nezobrazuje v rozhraní.

Výsledky kontroly IOC jsou uchovávány po dobu 30 dní. Po této době bude aplikace Kaspersky Endpoint Security automaticky odstraňovat nejstarší záznamy.

Rozšířená telemetrie pro Kontrolu IOC

Pro retrospektivní kontrolu IOC doporučujeme v počítači povolit rozšířenou telemetrii. Rozšířená telemetrie zlepšuje přesnost zjišťování IOC, ale využívá více prostředků počítače.

Rozšířená telemetrie zahrnuje podporu následujících dalších podmínek:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Je-li rozšířená telemetrie zakázána, Kaspersky Endpoint Security může střídat informace o zjištěných indikátorech narušení.

Postup povolení rozšířené telemetrie:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Zaškrtněte políčko **Enable advanced system activity logging**.
6. Uložte změny.

Přesunout soubor do karantény

Při reakci na hrozby může Kaspersky Endpoint Detection and Response vytvořit úlohu *Move file to Quarantine*. To je nezbytné pro minimalizaci následků hrozby. *Karanténa* je speciální místní úložiště v počítači. Uživatel může umístit do karantény soubory, které považuje za nebezpečné pro počítač. Soubory v karanténě jsou uloženy v šifrovaném stavu a neohrožují zabezpečení zařízení. Aplikace Kaspersky Endpoint Security použije karanténu, pouze je-li integrována s řešeními Kaspersky Detection and Response. V ostatních případech aplikace Kaspersky Endpoint Security umístí příslušný soubor do zálohy. Podrobnosti o správě karantény jako součásti řešení najdete v nápovědě k řešení Kaspersky Sandbox, nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum, nápovědě k řešení Kaspersky Endpoint Detection and Response Expert, nápovědě k řešení Kaspersky Anti Targeted Attack Platform a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise).

Úlohy *Move file to Quarantine* můžete vytvořit následujícími způsoby:

- V podrobnostech o výstraze (pouze EDR Optimum).

  Podrobnosti o výsledcích detekce je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

- Používání průvodce úlohami.

  Musíte zadat cestu k souboru nebo hodnotu hash (SHA256 nebo MD5) nebo cestu k souboru i hash souboru.

- V nastavení úlohy *IOC Scan*.

  Pokud úloha *IOC Scan* zjistí soubor, který může ohrozit data, můžete tento soubor umístit do karantény přímo ve výsledcích kontroly IOC (**Application settings** → **IOC Scan results**). Aplikace Kaspersky Endpoint Security tak spustí průvodce vytvořením úlohy s přednastavenými údaji o zjištěném souboru. Musíte pouze spravovat další nastavení úlohy, například nastavit plán úlohy.

Úloha *Move file to Quarantine* má následující omezení:

1. Velikost souboru nesmí překročit 100 MB.
2. Do karantény nelze umístit důležité systémové objekty (SCO). SCO jsou soubory, které operační systém a aplikace Kaspersky Endpoint Security pro systém Windows vyžadují k tomu, aby mohly fungovat.
3. Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.
4. Nemůžete kontrolovat objekt v karanténě v důsledku úlohy *Move file to Quarantine*.

Postup vytvoření úlohy Move file to Quarantine:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Move file to Quarantine**.

   c. Do pole **Task name** zadejte krátký popis.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Next**.
5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Klikněte na tlačítko **Next**.

   Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Kliknutím na tlačítko **Finish** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.
9. V seznamu souborů klikněte na **Add**.

   Spustí se průvodce přidáním souboru.

10. Chcete-li přidat soubor, musíte zadat úplnou cestu k souboru nebo hash i cestu.

    Pokud je soubor umístěn na síťové jednotce, zadejte cestu k souboru začínající `\\`, a nikoli písmenem jednotky. Například `\\server\shared_folder\file.exe`. Pokud cesta k souboru obsahuje písmeno síťové jednotky, může se zobrazit chyba *Soubor nebyl nalezen*.

11. V okně vlastností úlohy vyberte kartu **Schedule**.

12. Nakonfigurujte plán úloh.

    Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

13. Uložte změny.

14. Zaškrtněte políčko vedle úlohy.

15. Klikněte na tlačítko **Start**.

    Výsledkem je, že aplikace Kaspersky Endpoint Security přesune soubor do karantény.

Pokud je soubor uzamčen jiným procesem, úloha se zobrazí jako *Completed*, ale samotný soubor je uložen do karantény až po restartu počítače. Po restartování počítače potvrďte, že je soubor odstraněn.

Úloha *Move file to Quarantine* může skončit s chybou *Přístup odepřen*, pokud se pokoušíte uložit do karantény aktuálně spuštěný spustitelný soubor. Vytvořte pro soubor úlohu Ukončit proces a zkuste to znovu.

Úloha *Move file to Quarantine* může skončit s chybou *Nedostatek místa v úložišti karantény*, pokud se pokoušíte uložit do karantény soubor, který je příliš velký. Vyprázdněte karanténu nebo ji zvětšete. Poté akci opakujte.

Pomocí aplikace webové konzoly můžete obnovit soubor z karantény nebo karanténu vyprázdnit. Objekty můžete obnovit místně v počítači pomocí příkazového řádku.

Načíst soubor

Soubory můžete získat z uživatelských počítačů. Můžete například nakonfigurovat získání souboru protokolu událostí vytvořeného aplikací třetí strany. Po provedení úlohy je soubor uložen do karantény. *Karanténa* je speciální místní úložiště v počítači. Tento soubor si můžete stáhnout z karantény do počítače pomocí webové konzoly (**Operace** → **Úložiště** → **Karanténa**). V počítači uživatele zůstane soubor v původní složce.

Velikost souboru nesmí překročit 100 MB.

Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Postup vytvoření úlohy Načíst soubor:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Get file**.

   c. Do pole **Task name** zadejte krátký popis.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

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

5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Klikněte na tlačítko **Next**.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Kliknutím na tlačítko **Finish** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.

9. V seznamu souborů klikněte na **Add**.

   Spustí se průvodce přidáním souboru.

10. Chcete-li přidat soubor, musíte zadat úplnou cestu k souboru nebo hash i cestu.

    Pokud je soubor umístěn na síťové jednotce, zadejte cestu k souboru začínající `\\`, a nikoli písmenem jednotky. Například `\\server\shared_folder\file.exe`. Pokud cesta k souboru obsahuje písmeno síťové jednotky, může se zobrazit chyba *Soubor nebyl nalezen*.

11. V okně vlastností úlohy vyberte kartu **Schedule**.

12. Nakonfigurujte plán úloh.

    Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

13. Uložte změny.

14. Zaškrtněte políčko vedle úlohy.

15. Klikněte na tlačítko **Start**.

    Výsledkem je, že aplikace Kaspersky Endpoint Security vytvoří kopii souboru a přesune ji do karantény. Soubor z karantény si můžete stáhnout ve webové konzole.

Odstranit soubor

Soubory můžete vzdáleně odstraňovat pomocí úlohy *Delete file*. Při reakci na hrozby můžete například vzdáleně odstranit soubor.

Úloha *Delete file* má následující omezení:

- System Critical Object (SCO) nelze odstranit. SCO jsou soubory, které operační systém a aplikace Kaspersky Endpoint Security vyžadují k tomu, aby mohly fungovat.
- Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Postup vytvoření úlohy Delete file:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Delete file**.

   c. Do pole **Task name** zadejte krátký popis.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

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

5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Klikněte na tlačítko **Next**.

Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Kliknutím na tlačítko **Finish** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.

9. V seznamu souborů klikněte na **Add**.

   Spustí se průvodce přidáním souboru.

10. Chcete-li přidat soubor, musíte zadat úplnou cestu k souboru nebo hash i cestu.

    Pokud je soubor umístěn na síťové jednotce, zadejte cestu k souboru začínající `\\`, a nikoli písmenem jednotky. Například `\\server\shared_folder\file.exe`. Pokud cesta k souboru obsahuje písmeno síťové jednotky, může se zobrazit chyba *Soubor nebyl nalezen*.

11. V okně vlastností úlohy vyberte kartu **Schedule**.

12. Nakonfigurujte plán úloh.

    Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

13. Uložte změny.

14. Zaškrtněte políčko vedle úlohy.

15. Klikněte na tlačítko **Start**.

    Výsledkem je, že aplikace Kaspersky Endpoint Security odstraní soubor z počítače. Pokud je soubor uzamčen jiným procesem, úloha se zobrazí jako *Done*, ale samotný soubor je odstraněn až po restartu počítače. Po restartování počítače potvrďte, že je soubor odstraněn.

Úloha *Delete file* může skončit s chybou *Access denied or file not found*, pokud se pokoušíte odstranit aktuálně spuštěný spustitelný soubor. Vytvořte pro soubor úlohu Ukončit proces a zkuste to znovu.

Zahájení procesu

Soubory můžete vzdáleně spouštět pomocí úlohy *Process start*. Můžete například vzdáleně spustit nástroj, který vytvoří konfigurační soubor počítače. Dále můžete pomocí úlohy *Get file* přijmout vytvořený soubor ve webové konzole aplikace Kaspersky Security Center.

Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Postup vytvoření úlohy Process start:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Process start**.

   c. Do pole **Task name** zadejte krátký popis.

   d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

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

5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Klikněte na tlačítko **Next**.

   Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Kliknutím na tlačítko **Finish** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

8. Otevře se okno vlastností úlohy.

9. Vyberte kartu **Application settings**.

10. Zadejte příkaz pro zahájení procesu.

    Předpokládejme, že chcete spustit nástroj (`utility.exe`), který uloží informace o konfiguraci počítače do souboru s názvem `conf.txt` do aktuální složky (ve výchozím nastavení). Nástroj je ve složce `C:\Users\admin\Diagnostic\`. Konfigurační soubor musíte uložit do složky `C:\Users\admin\Documents\Configuration`. Zadejte následující hodnoty:

    - **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Command line arguments (optional)** – `/R conf.txt`
    - **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. V okně vlastností úlohy vyberte kartu **Schedule**.

12. Nakonfigurujte plán úloh.

    Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

13. Uložte změny.

14. Zaškrtněte políčko vedle úlohy.

15. Klikněte na tlačítko **Start**.

    Výsledkem je, že aplikace Kaspersky Endpoint Security spustí příkaz v bezobslužném režimu a spustí proces. Výsledky úlohy můžete zobrazit ve vlastnostech úlohy v části **Execution results**.

Ukončit proces

Procesy můžete vzdáleně ukončit pomocí úlohy *Terminate process*. Například můžete vzdáleně ukončit nástroj pro testování rychlosti internetu, který byl spuštěn pomocí úlohy *Spustit proces*.

Pokud chcete zakázat spouštění souboru, můžete nakonfigurovat součást Prevence spouštění. Můžete zakázat spouštění spustitelných souborů, skriptů, souborů ve formátu Office.

Úloha *Terminate process* má následující omezení:

- Nelze ukončit procesy důležitých systémových objektů (SCO). SCO jsou soubory, které operační systém a aplikace Kaspersky Endpoint Security vyžadují k tomu, aby mohly fungovat.
- Úlohu pro EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení úloh pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Postup vytvoření úlohy Terminate process:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na tlačítko **Add**.

   Spustí se průvodce úlohou.

3. Konfigurace nastavení úlohy:

   a. V rozevíracím seznamu **Application** vyberte možnost **Kaspersky Endpoint Security for Windows 14.0.0**.

   b. V rozevíracím seznamu **Task type** vyberte možnost **Terminate process**.

c. Do pole **Task name** zadejte krátký popis.

d. V bloku **Devices to which the task will be assigned** vyberte rozsah úlohy.

4. Vyberte zařízení podle vybrané možnosti rozsahu úlohy. Klikněte na tlačítko **Next**.
5. Zadejte přihlašovací údaje účtu uživatele, jehož práva chcete použít ke spuštění úlohy. Klikněte na tlačítko **Next**.

   Ve výchozím nastavení aplikace Kaspersky Endpoint Security spouští úlohu jako systémový uživatelský účet (SYSTEM).

6. Kliknutím na tlačítko **Finish** dokončete průvodce.

   V seznamu úloh se zobrazí nová úloha.

7. Klikněte na novou úlohu.

   Otevře se okno vlastností úlohy.

8. Vyberte kartu **Application settings**.
9. Chcete-li dokončit proces, musíte vybrat soubor, který chcete ukončit. Soubor lze vybrat jedním z následujících způsobů:

   - Zadejte celý název souboru.
   - Zadejte hash souboru a cestu k souboru.
   - Zadejte PID procesu (pouze pro místní úlohy).

   Pokud je soubor umístěn na síťové jednotce, zadejte cestu k souboru začínající `\\`, a nikoli písmenem jednotky. Například `\\server\shared_folder\file.exe`. Pokud cesta k souboru obsahuje písmeno síťové jednotky, může se zobrazit chyba *Soubor nebyl nalezen*.

10. V okně vlastností úlohy vyberte kartu **Schedule**.
11. Nakonfigurujte plán úloh.

    Funkce Wake-on-LAN není u této úlohy k dispozici. Aby bylo možné úlohu spustit, musí být počítač zapnutý.

12. Klikněte na tlačítko **Save**.
13. Zaškrtněte políčko vedle úlohy.
14. Klikněte na tlačítko **Start**.

    Výsledkem je, že aplikace Kaspersky Endpoint Security ukončí proces v počítači. Pokud je například spuštěna aplikace GAME a vy ukončíte proces game.exe, tato aplikace bude ukončena bez uložení dat. Výsledky úlohy můžete zobrazit ve vlastnostech úlohy v části **Results**.

Prevence spouštění

Prevence spouštění umožňuje spravovat spouštění spustitelných souborů a skriptů a také otevírání souborů formátu aplikací Office. Můžete tak například zabránit spuštění aplikací, které považujete za nebezpečné. Díky tomu lze šíření hrozby zastavit. Prevence spouštění podporuje sadu přípon kancelářských souborů a sadu interpretů skriptů.

Pravidlo prevence spouštění

Prevence spouštění spravuje přístup uživatele k souborům pomocí pravidel prevence spouštění. *Pravidlo prevence spouštění* je sada kritérií, která aplikace bere v úvahu při reakci na spuštění objektu, například při blokování spuštění objektu. Aplikace identifikuje soubory podle jejich cest nebo kontrolních součtů vypočítaných pomocí algoritmů hash MD5 a SHA256.

Pravidla prevence spouštění můžete vytvořit:

- V podrobnostech o výstraze (pouze EDR Optimum).

  Podrobnosti o výsledcích detekce je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

- Pomocí zásady skupiny nebo místního nastavení aplikace.

  Musíte zadat cestu k souboru nebo hodnotu hash (SHA256 nebo MD5) nebo cestu k souboru i hash souboru.

Prevenci spouštění můžete také lokálně povolit nebo zakázat pomocí příkazového řádku.

Prevence spouštění má následující omezení:

1. Pravidla prevence se nevztahují na soubory na CD ani bitových kopiích ISO. Aplikace neblokuje spouštění ani otevírání těchto souborů.
2. Není možné blokovat spouštění objektů kritických pro systém (SCO). SCO jsou soubory, které operační systém a aplikace Kaspersky Endpoint Security vyžadují k tomu, aby mohly fungovat.
3. Nedoporučujeme vytvářet více než 5000 pravidel prevence spouštění, protože to může způsobit nestabilitu systému.

Režimy pravidla prevence spouštění

Součást Prevence spouštění může fungovat ve dvou režimech:

- **Pouze statistika**

  V tomto režimu aplikace Kaspersky Endpoint Security publikuje událost o pokusech o spuštění spustitelných objektů nebo otevřených dokumentech, které odpovídají kritériím pravidel prevence do protokolu událostí systému Windows a Kaspersky Security Center, ale neblokuje pokus o spuštění nebo otevření objektu nebo dokumentu. Tento režim je ve výchozím nastavení vybrán.

- **Aktivní**

  V tomto režimu aplikace blokuje spouštění objektů nebo otevírání dokumentů, které odpovídají kritériím pravidla prevence. Aplikace také publikuje událost o pokusech o spuštění objektů nebo otevření dokumentů do protokolu událostí systému Windows a protokolu událostí aplikace Kaspersky Security Center.

Správa Prevence spouštění

Nastavení součásti můžete konfigurovat pouze ve webové konzole.

Postup prevence spouštění:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Vyberte kartu **Execution Prevention**.
6. Zapněte přepínač **Execution Prevention ENABLED**.
7. V bloku **Action on execution or opening of forbidden object** vyberte provozní režim součásti:

   - **Block and add to event log**. V tomto režimu aplikace blokuje spouštění objektů nebo otevírání dokumentů, které odpovídají kritériím pravidla prevence. Aplikace také publikuje událost o pokusech o spuštění objektů nebo otevření dokumentů do protokolu událostí systému Windows a protokolu událostí aplikace Kaspersky Security Center.
   - **Add to event log**. V tomto režimu aplikace Kaspersky Endpoint Security publikuje událost o pokusech o spuštění spustitelných objektů nebo otevřených dokumentech, které odpovídají kritériím pravidel prevence do protokolu událostí systému Windows a Kaspersky Security Center, ale neblokuje pokus o spuštění nebo otevření objektu nebo dokumentu. Tento režim je ve výchozím nastavení vybrán.
8. Postup vytvoření seznamu pravidel prevence spouštění:

   a. Klikněte na tlačítko **Add**.

   b. Otevře se okno; do tohoto okna zadejte název pravidle prevence spouštění (například *Aplikace A*).

   c. V rozevíracím seznamu **Type** vyberte objekt, který chcete blokovat: **Executable file**, **Script**, **Microsoft Office document**.

   Pokud vyberete nesprávný typ objektu, aplikace Kaspersky Endpoint Security soubor nebo skript neblokuje.

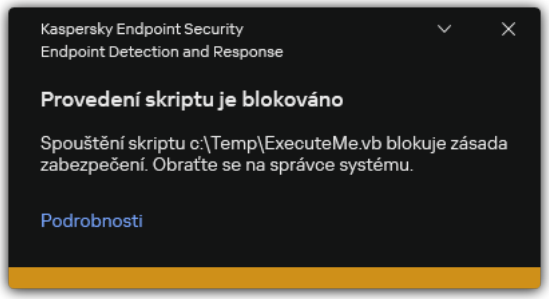
   d. Chcete-li přidat soubor, musíte zadat hash souboru (SHA256 nebo MD5), úplnou cestu k souboru nebo hash i cestu.

   Pokud je soubor umístěn na síťové jednotce, zadejte cestu k souboru začínající `\\`, a nikoli písmenem jednotky. Například `\\server\shared_folder\file.exe`. Pokud cesta k souboru obsahuje písmeno síťové jednotky, aplikace Kaspersky Endpoint Security příslušný soubor nebo skript neblokuje.

Prevence spouštění podporuje sadu přípon kancelářských souborů a sadu interpretů skriptů.

9. Uložte změny.

Výsledkem je, že aplikace Kaspersky Endpoint Security blokuje spouštění objektů: spouštění spustitelných objektů a skriptů, otevírání souborů ve formátu aplikací Office. Můžete ale například otevřít soubor skriptu v textovém editoru, i když je spouštění skriptu zabráněno. Při blokování spuštění objektu aplikace Kaspersky Endpoint Security zobrazí standardní upozornění (viz obrázek níže), pokud jsou v nastavení aplikace povolena upozornění.



Upozornění na prevenci spouštění

Izolace počítače od sítě

Izolace počítače od sítě umožňuje automaticky izolovat počítač od sítě v reakci na detekci indikátoru narušení (IOC) – to je *automatický režim*. Během zkoumání zjištěné hrozby můžete zapnout izolaci sítě ručně – to je *ruční režim*.

Když je funkce Izolace sítě zapnutá, aplikace přeruší všechna aktivní připojení a zablokuje všechna nová síťová připojení TCP/IP v počítači kromě následujících připojení:

- Připojení uvedená v části Výjimky z izolace sítě.
- Připojení iniciovaná službami Kaspersky Endpoint Security.
- Připojení iniciovaná součástí Kaspersky Security Center Network Agent.
- Připojení k SVM a integračního serveru, pokud je aplikace používána v režimu Light Agent.
- Připojení ke KSN při integraci aplikace s aplikací Kaspersky Managed Detection and Response.

Nastavení součásti můžete konfigurovat pouze ve webové konzole.

Automatický režim izolace sítě

Můžete nakonfigurovat, že se má funkce Izolace sítě zapínat automaticky v reakci na detekci IOC. Automatický režim izolace sítě můžete nakonfigurovat pomocí zásad skupiny.

Jak nakonfigurovat automatické zapínání funkce Izolace sítě v reakci na detekci IOC

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na úlohu **IOC Scan** Kaspersky Endpoint Security.
   Otevře se okno vlastností úlohy.
   V případě potřeby vytvořte úlohu *IOC Scan*.
3. Vyberte kartu **Application settings**.
4. V bloku **Action on IOC detection** zaškrtněte políčka **Take response actions after an IOC is found** a **Isolate computer from the network**.
5. Uložte změny.

Výsledkem je to, že pokud je zjištěn IOC, aplikace izoluje síť od sítě, aby se hrozba nemohla šířit.

Automatickou izolaci sítě můžete nakonfigurovat tak, aby byla po určité době zakázána. Ve výchozím nastavení aplikace vypne tuto funkci po uplynutí 8 hodin od jejího zapnutí. Izolaci sítě můžete také vypnout ručně (viz pokyny níže). Po vypnutí funkce Izolace sítě může počítač používat síť bez omezení.

Jak nakonfigurovat prodlevu pro vypnutí izolace počítače od sítě v automatickém režimu

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Vyberte kartu **Network Isolation**.
6. Vyberte prodlevu pro vypnutí Izolace sítě.
7. Uložte změny.

Ruční režim izolace sítě

Funkci Izolace sítě můžete zapnout nebo vypnout ručně. Ruční režim izolace sítě můžete nakonfigurovat pomocí vlastností počítače v konzole aplikace Kaspersky Security Center.

Funkci Izolace sítě můžete zapnout:

- V podrobnostech o výstraze (pouze EDR Optimum).
  Podrobnosti o výsledcích detekce je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.
- Pomocí místních nastavení aplikace.
- V nastavení úlohy *IOC Scan*.
  Pokud úloha *IOC Scan* zjistí IOC, můžete počítač izolovat od sítě přímo z IOC (vlastnosti úlohy *IOC Scan* → **Application settings** → **IOC Scan results**). Aplikace Kaspersky Endpoint Security také umožňuje okamžitou správu dalších nastavení: Doba zakázání izolace od sítě a Výjimky z izolace od sítě.

Jak ručně zapnout funkci izolaci počítače od sítě

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. Přejděte na **Detection and Response** → **Endpoint Detection and Response**.
7. V bloku **Network isolation** klikněte na **Isolate computer from the network**.

Automatickou izolaci sítě můžete nakonfigurovat tak, aby byla po určité době zakázána. Ve výchozím nastavení aplikace vypne tuto funkci po uplynutí 8 hodin od jejího zapnutí. Po vypnutí funkce Izolace sítě může počítač používat síť bez omezení.

Jak nakonfigurovat prodlevu pro vypnutí izolace počítače od sítě v ručním režimu

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.

3. Vyberte kartu **Tasks**.
   Zobrazí se seznam úloh dostupných v počítači.
4. Vyberte úlohu **Network isolation**.
5. Vyberte kartu **Application settings**.
6. Tím se otevře okno; v tomto okně vyberte prodlevu pro vypnutí izolace sítě.
7. Uložte změny.

Jak ručně vypnout funkci izolaci počítače od sítě

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. Přejděte na **Detection and Response** → **Endpoint Detection and Response**.
7. V bloku **Network isolation** klikněte na **Unblock computer isolated from the network**.

Izolaci sítě můžete také lokálně povolit nebo zakázat pomocí příkazového řádku.

Počínaje aplikací Kaspersky Endpoint Security 12.10 pro systém Windows můžete izolaci počítače od sítě spravovat v podrobnostech výstrahy. V podrobnostech výstrahy můžete navíc určit časové období izolace počítače od sítě. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

Výjimky z izolace sítě

Můžete nakonfigurovat výjimky z izolace sítě. Síťová připojení, která odpovídají pravidlům, nejsou na počítačích blokována, když je zapnutá izolace sítě.

Chcete-li nakonfigurovat výjimky z izolace sítě, můžete použít seznam *standardních síťových profilů*. Ve výchozím nastavení zahrnují výjimky síťové profily obsahující pravidla, která zajišťují nepřetržitý provoz zařízení s rolemi serveru DNS/DHCP a klienta DNS/DHCP. Můžete rovněž upravit nastavení standardních síťových profilů nebo výjimky definovat ručně (viz pokyny níže).

Výjimky uvedené ve vlastnostech zásad se použijí pouze v případě, že je izolace sítě automaticky zapnuta v reakci na zjištěnou hrozbu. Výjimky uvedené ve vlastnostech počítače se použijí pouze v případě, že je ve vlastnostech počítače v konzole Kaspersky Security Center nebo v podrobnostech o výstraze ručně zapnuta izolace sítě.

Aktivní zásada nebrání použití výjimek z izolace sítě nakonfigurovaných ve vlastnostech počítače, protože tyto parametry mají různé scénáře použití.

Jak přidat výjimku z izolace sítě v automatickém režimu

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Vyberte kartu **Network Isolation**.

6. V bloku **Network isolation exclusions** klikněte na **Exclusions**.
7. Otevře se okno; v tomto okně klikněte na možnost **Add** → **Add from profile** a vyberte standardní síťové profily pro konfiguraci výjimek.

   Výjimky z izolace sítě z profilu jsou přidány do seznamu výjimek z izolace sítě. Můžete zobrazit vlastnosti síťových připojení. V případě potřeby můžete nastavení síťových připojení upravit.
8. Pokud je potřeba, přidejte výjimku z izolace sítě ručně. To provedete tak, že v okně se seznamem výjimek kliknete na tlačítko **Add** → **Add** a ručně upravíte nastavení síťových připojení.
9. Uložte změny.

Jak přidat výjimku z izolace sítě v ručním režimu

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.

   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Tasks**.

   Zobrazí se seznam úloh dostupných v počítači.
4. Vyberte úlohu **Network isolation**.
5. Vyberte kartu **Application settings**.
6. Tím se otevře okno; v tomto okně klikněte na **Exclusions**.
7. Otevře se okno; v tomto okně klikněte na možnost **Add from profile** a vyberte standardní síťové profily pro konfiguraci výjimek.

   Výjimky z izolace sítě z profilu jsou přidány do seznamu výjimek z izolace sítě. Můžete zobrazit vlastnosti síťových připojení. V případě potřeby můžete nastavení síťových připojení upravit.
8. Pokud je potřeba, přidejte výjimku z izolace sítě ručně. To provedete tak, že v okně se seznamem výjimek kliknete na tlačítko **Add** a ručně upravíte nastavení síťových připojení.
9. Uložte změny.

Seznam výjimek z izolace sítě můžete rovněž zobrazit místně pomocí příkazového řádku. V tomto případě musí být počítač izolovaný.

Počínaje aplikací Kaspersky Endpoint Security 12.10 pro systém Windows můžete výjimky z izolace počítače od sítě spravovat v podrobnostech výstrahy. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

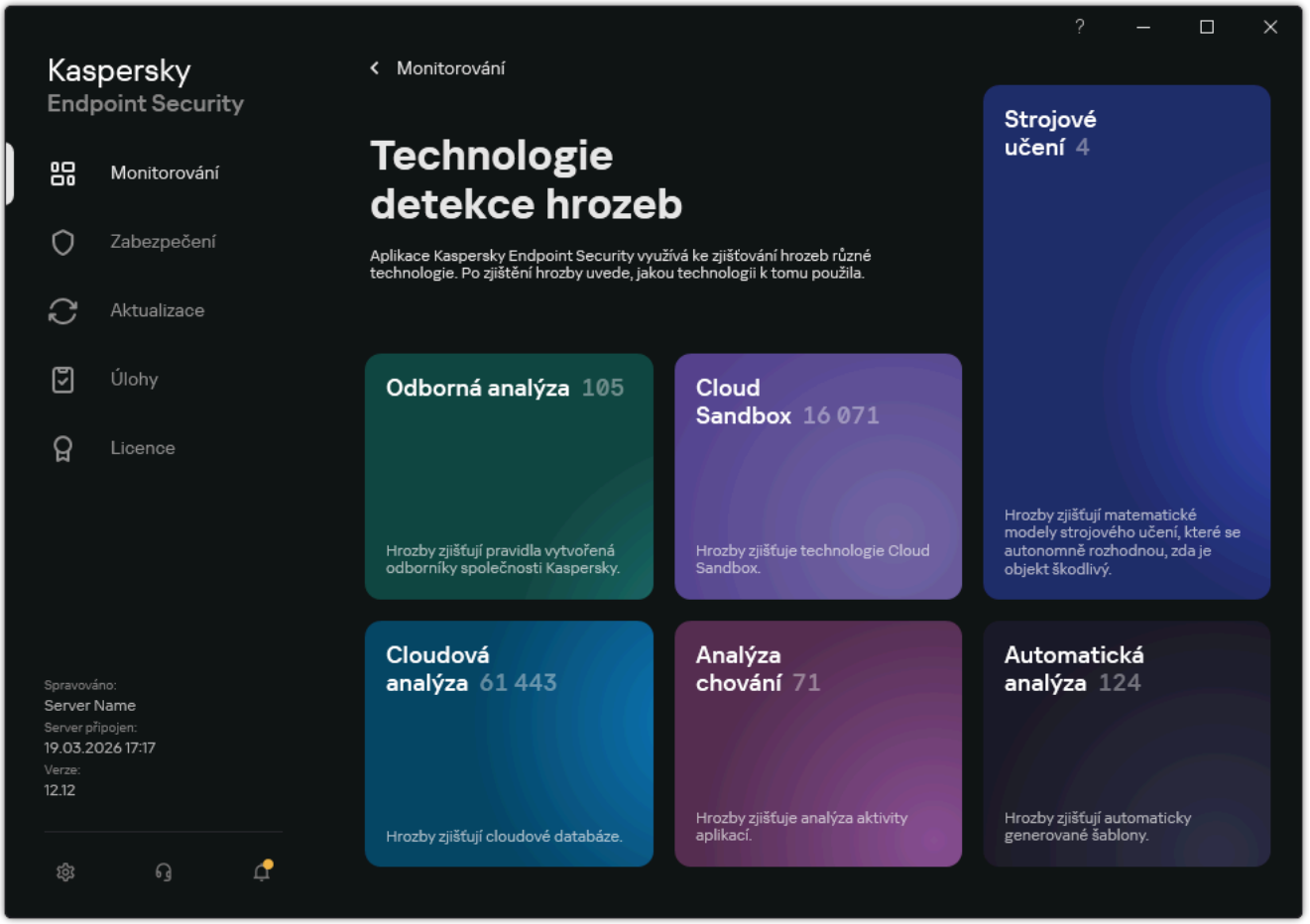
Cloud Sandbox

Cloud Sandbox je technologie, která vám umožňuje v počítači detekovat pokročilé hrozby. Kaspersky Endpoint Security automaticky předává zjištěné soubory do Cloud Sandboxu na analýzu. Cloud Sandbox tyto soubory spustí v izolovaném prostředí, aby zjistil škodlivou aktivitu, a rozhodne o jejich reputaci. Údaje o těchto souborech jsou poté odeslány do služby Kaspersky Security Network. Pokud Cloud Sandbox zjistí škodlivý soubor, aplikace Kaspersky Endpoint Security provede příslušnou akci, aby tuto hrozbu eliminovala ve všech počítačích, kde je tento soubor zjištěn.

Aby mohla technologie Cloud Sandbox fungovat, musíte povolit používání služby Kaspersky Security Network.

Pokud používáte Kaspersky Private Security Network, technologie Cloud Sandbox není k dispozici.

Technologie Cloud Sandbox je trvale povolena a je k dispozici všem uživatelům služby Kaspersky Security Network bez ohledu na typ licence, který používají. Pokud jste už nasadili řešení Endpoint Detection and Response (EDR Optimum nebo EDR Expert), můžete povolit samostatné počítadlo hrozeb zjištěných technologií Cloud Sandbox. Toto počítadlo můžete použít k vytváření statistik při analýze zjištěných hrozeb.



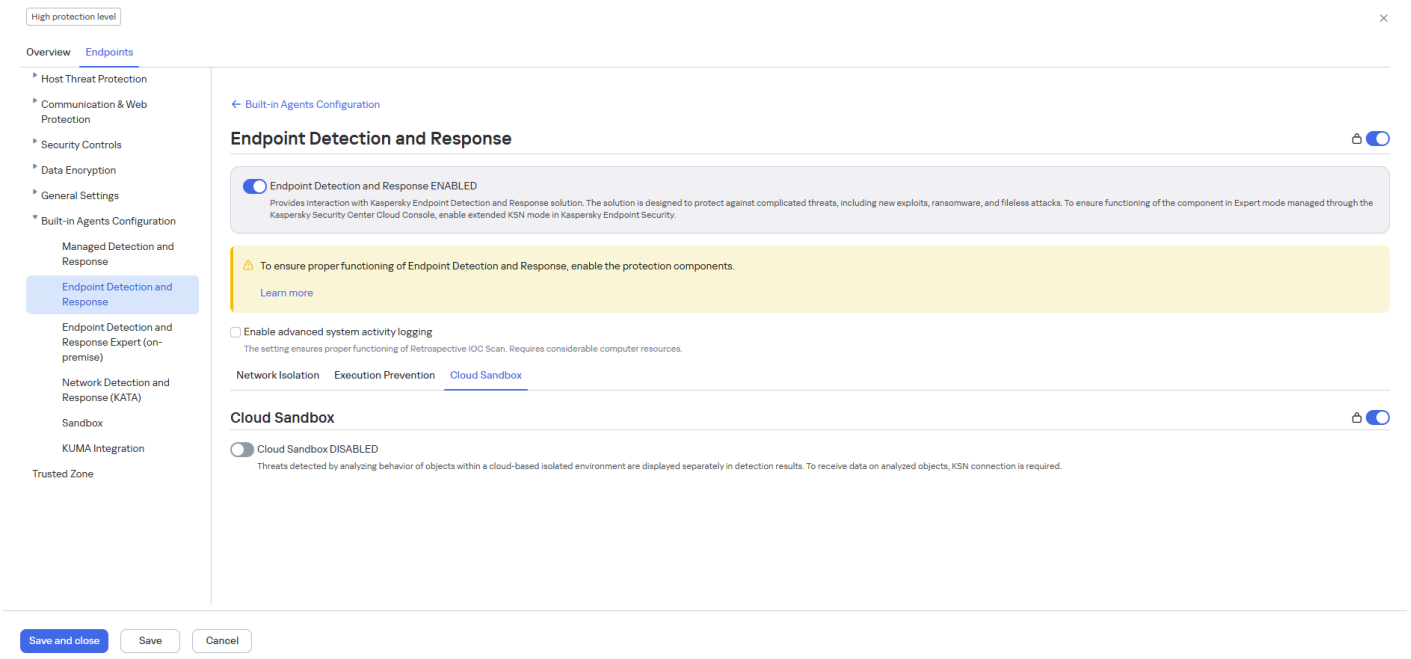
Počítadla hrozeb

Postup povolení počítadla pro Cloud Sandbox:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Vyberte kartu **Cloud Sandbox**.
6. Zapněte přepínač **Cloud Sandbox ENABLED**.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Kdykoli se vyskytne hrozba, aplikace Kaspersky Endpoint Security aktivuje počítadlo u hrozeb zjištěných pomocí technologie Cloud Sandbox v hlavním okně aplikace v části **Technologie detekce hrozeb**. Aplikace Kaspersky Endpoint Security bude technologii detekce hrozeb Cloud Sandbox uvádět také v části *Report on threats* v konzole aplikace Kaspersky Security Center.



Oddíl zásad Endpoint Detection and Response

Průvodce migrací KEA na KES pro EDR Optimum

Aplikace Kaspersky Endpoint Security pro systém Windows integrovaného agenta pro řešení Kaspersky Endpoint Detection and Response Optimum. Pro práci s řešením EDR Optimum už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent. Všechny funkce aplikace Kaspersky Endpoint Agent bude provádět aplikace Kaspersky Endpoint Security.

Když nasadíte Kaspersky Endpoint Security do počítačů s nainstalovanou aplikací Kaspersky Endpoint Agent, řešení Kaspersky Endpoint Detection and Response Optimum bude nadále fungovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent. Ke stejnému chování v systému dojde, když aktualizujete Kaspersky Endpoint Security na verzi 11.7.0 nebo novější.

Aplikace Kaspersky Endpoint Security není kompatibilní s aplikací Kaspersky Endpoint Agent. Obě tyto aplikace nelze nainstalovat do stejného počítače.

Aby aplikace Kaspersky Endpoint Security fungovala jako součást řešení Kaspersky Endpoint Detection and Response Optimum, musí být splněny následující podmínky:

- Kaspersky Endpoint Detection and Response Optimum verze 2.0 a novější.
- Kaspersky Security Center verze 13.2 nebo vyšší (včetně součásti Network Agent). Ve starších verzích aplikace Kaspersky Security Center není možné funkci EDR Optimum aktivovat.
- EDR Optimum lze spravovat pouze pomocí webové konzoly aplikace Kaspersky Security Center.
- Přenos dat na server pro správu je povolen. Tato data jsou nutná k získání informací o souborech umístěných do karantény na počítači prostřednictvím webové konzoly.
- Je navázáno připojení na pozadí mezi webovou konzolou aplikace Kaspersky Security Center a serverem pro správu. Aby součást EDR Optimum fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*.

Kroky pro migraci konfigurace [KES+KEA] na [KES+integrovaný agent] pro EDR Optimum

1. **Upgrade webového pluginu Kaspersky Endpoint Security**

   Součást EDR Optimum lze spravovat pomocí modulu plug-in pro správu aplikace Kaspersky Endpoint Security verze 11.7.0 nebo novější.

2. **Migrace zásady a úloh**

   Nastavení aplikace Kaspersky Endpoint Agent můžete přenést do aplikace Kaspersky Endpoint Security pro Windows. Chcete-li to provést, použijte průvodce migrací z aplikace Kaspersky Endpoint Agent ve webové konzole.

   Jak migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security ve webové konzole

   V hlavním okně webové konzoly vyberte možnosti **Operations** → **Migration from Kaspersky Endpoint Agent**.

Tím spustíte průvodce migrací zásad a úloh. Postupujte podle pokynů průvodce.

Krok 1. Migrace zásad

Průvodce migrací vytvoří novou zásadu, která sloučí nastavení zásad aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete sloučit se zásadami aplikace Kaspersky Endpoint Security. Kliknutím na zásadu aplikace Kaspersky Endpoint Agent vyberte zásadu aplikace Kaspersky Endpoint Security, s níž chcete sloučit nastavení. Zkontrolujte, zda jste vybrali správné zásady, a přejděte k dalšímu kroku.

Krok 2. Migrace úloh

Nové úlohy pro aplikaci Kaspersky Endpoint Security vytvoří průvodce migrací. V seznamu úloh vyberte úlohy aplikace Kaspersky Endpoint Agent, které chcete vytvořit pro zásady aplikace Kaspersky Endpoint Security. Přejděte k dalšímu kroku.

Krok 3. Dokončení průvodce

Ukončete průvodce. Průvodce tak provede následující:

- Vytvoří novou zásadu aplikace Kaspersky Endpoint Security.

  V zásadě se sloučí nastavení z aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Název zásady je *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Nová zásada má stav *Inactive*. Chcete-li pokračovat, změňte stav zásad aplikací Kaspersky Endpoint Agent a Kaspersky Endpoint Security na *Inactive* a aktivujte novou sloučenou zásadu.

  Po migraci z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security pro systém Windows zkontrolujte, zda má nová zásada nastavenu funkci přenosu dat na server pro správu (data souborů v karanténě a údaje o řetězci vývoje hrozeb). Hodnoty parametrů přenosu dat nejsou ze zásady aplikace Kaspersky Endpoint Agent migrovány.

- Vytvoří nové úlohy aplikace Kaspersky Endpoint Security.

  Nové úlohy jsou kopiemi úloh aplikace Kaspersky Endpoint Agent. Zároveň ponechá průvodce úlohy aplikace Kaspersky Endpoint Agent beze změny.

3 Licence k funkci EDR Optimum

Pokud používáte k aktivaci aplikací Kaspersky Endpoint Security pro systém Windows a Kaspersky Endpoint Agent společnou licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security, funkce EDR Optimum bude aktivována automaticky po upgradu aplikace na verzi 11.7.0 nebo novější. Nemusíte dělat nic jiného.

Jestliže používáte k aktivaci funkce EDR Optimum licenci k doplňku Kaspersky Endpoint Detection and Response Optimum, do úložiště aplikace Kaspersky Security Center se přidá klíč k EDR Optimum je povolena automatická distribuce licenčního klíče. Po upgradu aplikace na verzi 11.7.0 nebo novější je funkce EDR Optimum aktivována automaticky.

Pokud používáte k aktivaci aplikace Kaspersky Endpoint Agent licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security a jinou licenci k aktivaci Kaspersky Endpoint Security pro systém Windows, musíte nahradit klíč k aplikaci Kaspersky Endpoint Security pro systém Windows společným klíčem k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security. Klíč můžete nahradit pomocí úlohy *Add key*.

4 Instalace/upgrade aplikace Kaspersky Endpoint Security

Pro migraci funkce EDR Optimum během instalace nebo upgradu aplikace se doporučuje použít úlohu vzdálené instalace. Při vytváření úlohy vzdálené instalace je třeba v nastavení instalačního balíčku vybrat součást EDR Optimum.

Aplikaci můžete také upgradovat následujícími způsoby:

- Pomocí aktualizační služby Kaspersky.
- Místně pomocí průvodce instalací.

Aplikace Kaspersky Endpoint Security podporuje automatický výběr součástí při upgradu aplikace na počítači, na němž je nainstalována aplikace Kaspersky Endpoint Agent. Automatický výběr součástí závisí na oprávněních uživatelského účtu, který aplikaci upgraduje.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru EXE nebo MSI pod systémovým účtem (SYSTEM), Kaspersky Endpoint Security získá přístup k aktuálním licencím řešení Kaspersky. Pokud je tedy v počítači nainstalována například aplikace Kaspersky Endpoint Agent a aktivováno řešení EDR Optimum, instalační program aplikace Kaspersky Endpoint Security automaticky nakonfiguruje sadu součástí a vybere součást EDR Optimum. Tím se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent. Spuštění instalačního programu MSI pod systémovým účtem (SYSTEM) se obvykle provádí při upgradu prostřednictvím aktualizační služby Kaspersky nebo při nasazování instalačního balíčku prostřednictvím aplikace Kaspersky Security Center.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru MSI pod uživatelským účtem bez oprávnění, Kaspersky Endpoint Security nemá přístup k aktuálním licencím řešení Kaspersky. V tomto případě Kaspersky Endpoint Security automaticky vybere součásti na základě konfigurace Kaspersky Endpoint Agent. Poté se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent.

Kaspersky Endpoint Security podporuje upgrade bez restartování počítače. Režim upgradu aplikace můžete vybrat ve vlastnostech zásad.

5. **Kontrola chodu aplikace**

   Pokud je po instalaci nebo upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

   - Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
   - Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*. Pokud je stav součásti *Není součástí licence*, ujistěte se, že jste aktivovali funkci integrovaného agenta.
   - V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.

Kaspersky Sandbox



Aplikace Kaspersky Endpoint Security pro systém Windows obsahuje integrovaného agenta pro integraci s řešením Kaspersky Sandbox. Součást *Sandbox* detekuje a automaticky blokuje pokročilé hrozby na počítačích. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Podrobnosti o tomto řešení najdete v nápovědě k součásti Kaspersky Sandbox a nápovědě k řešení Kaspersky Anti Targeted Attack Platform.

Integrace integrovaného agenta s řešením Kaspersky Sandbox

Pro integraci se součástí Sandbox je vyžadováno přidání Kaspersky Sandbox. Součást Sandbox můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

Abyste mohli součást používat, musí být splněny následující podmínky:

- Kaspersky Security Center 13.2. Starší verze této aplikace neumožňují v případě reakce na hrozbu vytváření samostatných úloh Kontrola IOC.
- Součást lze spravovat pouze pomocí webové konzoly. Tuto součást nemůžete spravovat pomocí konzoly pro správu (MMC).
- Je aktivována aplikace a na její funkčnost se vztahuje licence.
- Přenos dat na server pro správu je povolen.

  Chcete-li používat všechny funkce řešení Kaspersky Sandbox, musí být povolen přenos dat o souborech v karanténě. Tato data jsou nutná k získání informací o souborech umístěných do karantény na počítači prostřednictvím webové konzoly. Můžete si například stáhnout soubor z karantény za účelem analýzy ve webové konzole.

  Jak povolit přenos dat na server pro správu ve webové konzole

  1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
  2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

     Otevře se okno vlastností zásad.
  3. Vyberte kartu **Application settings**.
  4. Přejděte na **General Settings** → **KSC Integration**.
  5. V bloku **Data transfer to Administration Server** zaškrtněte políčko **About Quarantine files**.
  6. Uložte změny.

- Je navázáno připojení na pozadí mezi webovou konzolou aplikace Kaspersky Security Center a serverem pro správu

  Aby součást Kaspersky Sandbox fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*. Podrobnosti o integraci aplikace Kaspersky Security Center s ostatními řešeními společnosti Kaspersky najdete v nápovědě k aplikaci Kaspersky Security Center.

  Navázání připojení na pozadí ve webové konzole

  1. V hlavním okně webové konzoly vyberte možnosti **Settings** → **Integration**.
  2. Přejděte do části **Integration**.
  3. Zapněte přepínač **Background connection for integration Enabled**.

4. Uložte změny.

Není-li navázáno připojení na pozadí mezi webovou konzolou aplikace Kaspersky Security Center a serverem pro správu, v rámci reakce na hrozbu nelze vytvářet samostatné úlohy kontroly IOC.

- Chcete-li konfigurovat důvěryhodné připojení k serveru Sandbox, musíte si připravit certifikát TLS. Poté musíte přidat certifikát do počítače pomocí zásady. Musíte také přidat certifikát na server Sandbox.

  Ověření na obou stranách pomocí kryptokontejneru není pro Kaspersky Sandbox dostupné.

  Certifikát TLS můžete také přidat ve webové konzole nebo lokálně pomocí příkazového řádku.

- Je povolena součást Kaspersky Sandbox.
- Součásti aplikace, které zajišťují provoz součásti Sandbox, jsou povoleny a funkční. Provoz součásti Sandbox zajišťují následující součásti:
  - Ochrana před souborovými hrozbami.
  - Prevence narušení hostitele.
  - Brána firewall.
  - Ochrana AMSI.
  - Kontrola na pozadí.

Postup povolení nebo zakázání integrace s řešením Kaspersky Sandbox:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Sandbox**.
5. Pomocí přepínače **Integration with Sandbox ENABLED** můžete tuto součást povolit nebo zakázat.
6. V bloku **Integration mode** vyberte provozní režim součásti: **Kaspersky Sandbox**.
7. Klikněte na odkaz **Connection settings**.
   Tím se otevře okno nastavení připojení k serveru Sandbox.
8. V bloku **Server TLS certificate** klikněte na **Upload** a vyberte soubor certifikátu TLS.
   Kaspersky Endpoint Security může mít pro server Sandbox pouze jeden certifikát TLS. Pokud jste již dříve přidali certifikát TLS, bude tento certifikát odvolán. Používá se pouze poslední přidaný certifikát.
9. Konfigurace pokročilých nastavení připojení pro servery Sandbox:
   - **Timeout (msec)**. Časový limit připojení pro server Sandbox. Po uplynutí nastaveného časového limitu odešle aplikace Kaspersky Endpoint Security požadavek na další server. Pokud je rychlost připojení nízká nebo je připojení nestabilní, můžete prodloužit časový limit připojení pro server. Doporučovaný časový limit požadavku je 0,5 sekundy a méně.
   - **Request queue**. Velikost složky fronty žádostí. Při odesílání více objektů ke kontrole v součásti Sandbox vytvoří Kaspersky Endpoint Security frontu požadavků. Ve výchozím nastavení je velikost složky fronty žádostí omezena na 100 MB. Jakmile je dosaženo maximální velikosti, Sandbox přestane přidávat nové žádosti do fronty a odešle odpovídající událost do aplikace Kaspersky Security Center. Velikost složky fronty žádostí můžete konfigurovat v závislosti na konfiguraci serveru.
10. V bloku **Connection to Sandbox servers** klikněte na tlačítko **Add**.
11. Otevře se okno; v okně zadejte adresu a port serveru součásti Sandbox (IPv4, IPv6, DNS).
    Podrobnosti o nasazení virtuálních bitových kopií a konfiguraci serverů Sandbox najdete v nápovědě k řešení Kaspersky Sandbox.
12. Uložte změny.

Kaspersky Endpoint Security tak ověří certifikát TLS. Pokud je certifikát úspěšně ověřen, aplikace Kaspersky Endpoint Security soubor nahraje soubor certifikátu do počítače během další synchronizace s aplikací Kaspersky Security Center. Pokud jste přidali dva certifikáty TLS, Kaspersky Sandbox použije k navázání důvěryhodného připojení nejnovější certifikát. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Sandbox** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Integraci s řešením Kaspersky Sandbox můžete povolit nebo zakázat ve webové konzole nebo lokálně pomocí příkazového řádku.

Kaspersky Endpoint Security ukládá informace o fungování součásti Kaspersky Sandbox do zprávy. Zpráva také obsahuje informace o chybách. Pokud se zobrazí chyba s popisem, který odpovídá formátu `Error code: XXX` (např. `0xa67b01f4`), kontaktujte technickou podporu.

Vyhledávání indikátorů narušení (samostatná úloha)

Indikátor narušení (IOC) je sada dat o objektu nebo činnosti, která indikuje neoprávněný přístup k počítači (narušení dat). Indikátor narušení může například představovat mnoho neúspěšných pokusů o přihlášení do systému. Úloha *IOC Scan* umožňuje v počítači najít tyto indikátory narušení a přijmout opatření jako reakci na hrozby.

Kaspersky Endpoint Security vyhledává indikátory narušení pomocí souborů IOC. *Soubory IOC* jsou soubory obsahující sady indikátorů, které se aplikace pokusí porovnat, aby započítala detekci. Soubory IOC musí odpovídat standardu OpenIOC. Kaspersky Endpoint Security automaticky generuje soubory IOC pro řešení Kaspersky Sandbox.

Režim spuštění úlohy IOC Scan

Aplikace vytváří samostatné úlohy kontroly IOC pro řešení Kaspersky Sandbox. *Samostatná úloha kontroly IOC* je skupinová úloha, která se automaticky vytvoří při reakci na hrozbu detekovanou řešením Kaspersky Sandbox. Kaspersky Endpoint Security automaticky vygeneruje soubor IOC. Vlastní soubory IOC nejsou podporovány. Úlohy jsou automaticky odstraněny 30 dní po vytvoření. Další podrobnosti o samostatných úlohách kontroly IOC najdete v nápovědě k řešení Kaspersky Sandbox.

Nastavení úlohy IOC Scan

Kaspersky Sandbox může v reakci na hrozby automaticky vytvářet a spouštět úlohy *IOC Scan*.

Nastavení můžete konfigurovat pouze ve webové konzole.

Aby fungovaly samostatné úlohy kontroly řešení Kaspersky Sandbox, potřebujete aplikaci Kaspersky Security Center verze 13.2.

Postup změny nastavení úlohy IOC Scan:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Tasks**.

   Otevře se seznam úloh.

2. Klikněte na úlohu **IOC Scan** Kaspersky Endpoint Security.

   Otevře se okno vlastností úlohy.

3. Vyberte kartu **Application settings**.

4. Přejděte do části **IOC Scan settings**.

5. Konfigurace akcí při detekci IOC:

   - **Move copy to Quarantine, delete object**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security odstraní škodlivý objekt nalezený v počítači. Před odstraněním objektu vytvoří aplikace Kaspersky Endpoint Security záložní kopii pro případ, že bude nutné objekt později obnovit. Kaspersky Endpoint Security přesune záložní kopii do karantény.

   - **Run Critical Areas Scan**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security spustí úlohu *Kontrola kritických oblastí*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků.

   - **Run only when the computer is idle**. Odložené spuštění úlohy, když jsou prostředky počítače zaneprázdněny. Aplikace Kaspersky Endpoint Security spustí úlohu kontroly, pokud je počítač uzamčen nebo je zapnutý spořič obrazovky. Pokud jste přerušili provádění úlohy, například odemknutím počítače, aplikace Kaspersky Endpoint Security úlohu automaticky spustí a pokračuje od bodu, kde byla přerušena. Tato možnost plánování vám umožňuje šetřit prostředky počítače, když je počítač používán.

6. Uložte změny.

Výsledky úlohy můžete zobrazit ve vlastnostech úlohy v části **Results**. Informace o zjištěných indikátorech narušení můžete zobrazit ve vlastnostech úlohy: **Application settings** → **IOC Scan results**.

Výsledky kontroly IOC jsou uchovávány po dobu 30 dní. Po této době bude aplikace Kaspersky Endpoint Security automaticky odstraňovat nejstarší záznamy.

Průvodce migrací KEA na KES pro Kaspersky Sandbox

Aplikace Kaspersky Endpoint Security pro systém Windows integrovaného agenta pro řešení Kaspersky Sandbox. Pro práci s řešením Kaspersky Sandbox už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent. Všechny funkce aplikace Kaspersky Endpoint Agent bude provádět aplikace Kaspersky Endpoint Security.

Když nasadíte Kaspersky Endpoint Security do počítačů s nainstalovanou aplikací Kaspersky Endpoint Agent, řešení Kaspersky Sandbox bude nadále fungovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent. Ke stejnému chování v systému dojde, když aktualizujete Kaspersky Endpoint Security na verzi 11.7.0 nebo novější.

Aplikace Kaspersky Endpoint Security není kompatibilní s aplikací Kaspersky Endpoint Agent. Obě tyto aplikace nelze nainstalovat do stejného počítače.

Aby aplikace Kaspersky Endpoint Security fungovala jako součást řešení Kaspersky Sandbox, musí být splněny následující podmínky:

- Kaspersky Sandbox verze 2.0 nebo vyšší.
- Kaspersky Security Center verze 13.2 nebo vyšší (včetně součásti Network Agent). Ve starších verzích aplikace Kaspersky Security Center není možné funkci Kaspersky Sandbox aktivovat.
- Kaspersky Sandbox lze spravovat pouze pomocí webové konzoly aplikace Kaspersky Security Center.
- Přenos dat na server pro správu je povolen. Tato data jsou nutná k získání informací o souborech umístěných do karantény na počítači prostřednictvím webové konzoly.
- Je navázáno připojení na pozadí mezi webovou konzolou aplikace Kaspersky Security Center a serverem pro správu. Aby součást Kaspersky Sandbox fungovala se serverem pro správu prostřednictvím webové konzoly aplikace Kaspersky Security Center, musíte navázat nové bezpečné připojení, *připojení na pozadí*.

Kroky pro migraci konfigurace [KES+KEA] na [KES+integrovaný agent] pro Kaspersky Sandbox

1. **Upgrade webového pluginu Kaspersky Endpoint Security**

   Součást Kaspersky Sandbox lze spravovat pomocí webového modulu plug-in aplikace Kaspersky Endpoint Security verze 11.7.0 nebo novější.

2. **Migrace zásady a úloh**

   Nastavení aplikace Kaspersky Endpoint Agent můžete přenést do aplikace Kaspersky Endpoint Security pro Windows. Chcete-li to provést, použijte průvodce migrací z aplikace Kaspersky Endpoint Agent ve webové konzole.

   Jak migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security ve webové konzole

   V hlavním okně webové konzoly vyberte možnosti **Operations → Migration from Kaspersky Endpoint Agent**.

   Tím spustíte průvodce migrací zásad a úloh. Postupujte podle pokynů průvodce.

   Krok 1. Migrace zásad

   Průvodce migrací vytvoří novou zásadu, která sloučí nastavení zásad aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete sloučit se zásadami aplikace Kaspersky Endpoint Security. Kliknutím na zásadu aplikace Kaspersky Endpoint Agent vyberte zásadu aplikace Kaspersky Endpoint Security, s níž chcete sloučit nastavení. Zkontrolujte, zda jste vybrali správné zásady, a přejděte k dalšímu kroku.

   Krok 2. Migrace úloh

   Nové úlohy pro aplikaci Kaspersky Endpoint Security vytvoří průvodce migrací. V seznamu úloh vyberte úlohy aplikace Kaspersky Endpoint Agent, které chcete vytvořit pro zásady aplikace Kaspersky Endpoint Security. Přejděte k dalšímu kroku.

   Krok 3. Dokončení průvodce

   Ukončete průvodce. Průvodce tak provede následující:

   - Vytvoří novou zásadu aplikace Kaspersky Endpoint Security.

     V zásadě se sloučí nastavení z aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Název zásady je *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Nová zásada má stav *Inactive*. Chcete-li pokračovat, změňte stav zásad aplikací Kaspersky Endpoint Agent a Kaspersky Endpoint Security na *Inactive* a aktivujte novou sloučenou zásadu.

Po migraci z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security pro systém Windows zkontrolujte, zda má nová zásada nastavenu funkci přenosu dat na server pro správu (data souborů v karanténě a údaje o řetězci vývoje hrozeb). Hodnoty parametrů přenosu dat nejsou ze zásady aplikace Kaspersky Endpoint Agent migrovány.

- Vytvoří nové úlohy aplikace Kaspersky Endpoint Security.

  Nové úlohy jsou kopiemi úloh aplikace Kaspersky Endpoint Agent. Zároveň ponechá průvodce úlohy aplikace Kaspersky Endpoint Agent beze změny.

3. **Licencování funkcí součásti Kaspersky Sandbox**

   Chcete-li aktivovat Kaspersky Endpoint Security jako součást řešení Kaspersky Sandbox, potřebujete samostatnou licenci pro doplněk Kaspersky Sandbox. Klíč můžete přidat pomocí úlohy *Add key*. Do aplikace tak budou přidány dva klíče: *Kaspersky Endpoint Security* a *Kaspersky Sandbox*.

4. **Instalace/upgrade aplikace Kaspersky Endpoint Security**

   Pro migraci součásti Kaspersky Sandbox během instalace nebo upgradu aplikace se doporučuje použít úlohu vzdálené instalace. Při vytváření úlohy vzdálené instalace je třeba v nastavení instalačního balíčku vybrat součást Kaspersky Sandbox.

   Aplikaci můžete také upgradovat následujícími způsoby:

   - Pomocí aktualizační služby Kaspersky.
   - Místně pomocí průvodce instalací.

   Aplikace Kaspersky Endpoint Security podporuje automatický výběr součástí při upgradu aplikace na počítači, na němž je nainstalována aplikace Kaspersky Endpoint Agent. Automatický výběr součástí závisí na oprávněních uživatelského účtu, který aplikaci upgraduje.

   Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru EXE nebo MSI pod systémovým účtem (SYSTEM), Kaspersky Endpoint Security získá přístup k aktuálním licencím řešení Kaspersky. Pokud je tedy v počítači nainstalována například aplikace Kaspersky Endpoint Agent a aktivováno řešení Kaspersky Sandbox, instalační program aplikace Kaspersky Endpoint Security automaticky nakonfiguruje sadu součástí a vybere součást EDR Optimum. Tím se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent. Spuštění instalačního programu MSI pod systémovým účtem (SYSTEM) se obvykle provádí při upgradu prostřednictvím aktualizační služby Kaspersky nebo při nasazování instalačního balíčku prostřednictvím aplikace Kaspersky Security Center.

   Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru MSI pod uživatelským účtem bez oprávnění, Kaspersky Endpoint Security nemá přístup k aktuálním licencím řešení Kaspersky. V tomto případě Kaspersky Endpoint Security automaticky vybere součásti na základě konfigurace Kaspersky Endpoint Agent. Poté se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent.

   Kaspersky Endpoint Security podporuje upgrade bez restartování počítače. Režim upgradu aplikace můžete vybrat ve vlastnostech zásad.

5. **Kontrola chodu aplikace**

   Pokud je po instalaci nebo upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

   - Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
   - Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*. Pokud je stav součásti *Není součástí licence*, ujistěte se, že jste aktivovali funkci integrovaného agenta.
   - V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.

Kaspersky Anti Targeted Attack Platform



Kaspersky Endpoint Security pro systém Windows podporuje práci s řešením Kaspersky Anti Targeted Attack Platform (EDR (KATA)). 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. Kaspersky Anti Targeted Attack Platform obsahuje tři funkční jednotky:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Všechny funkční jednotky nebo jednotlivé funkční jednotky můžete zakoupit samostatně. Podrobnosti o tomto řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform. Aplikace obsahuje integrované agenty pro součásti EDR, NDR. Aplikace také podporuje práci se součástí Sandbox, která je součástí KATA.

Nástroje Threat Intelligence

Kaspersky Endpoint Detection and Response používá tyto nástroje po potlačování bezpečnostních hrozeb (Threat Intelligence):

- Integrace s portálem Kaspersky Threat Intelligence Portal, který obsahuje a zobrazuje informace o reputaci souborů a adres URL.
- Databáze Kaspersky Threats.
- Infrastruktura cloudových služeb Kaspersky Security Network (dále také jen „KSN"), která poskytuje přístup k informacím o souborech, webových stránkách a reputaci softwaru v reálném čase ze znalostní báze společnosti Kaspersky. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikací společnosti Kaspersky na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků.

Princip fungování řešení

Aplikace Kaspersky Endpoint Security se instaluje na jednotlivé počítače v podnikové IT infrastruktuře a nepřetržitě sleduje procesy, otevřená síťová připojení a upravované soubory. Informace o událostech v počítači (telemetrická data) jsou odesílány na server Kaspersky Anti Targeted Attack Platform. V tomto případě aplikace Kaspersky Endpoint Security také odešle na server Kaspersky Anti Targeted Attack Platform informace o hrozbách objevených aplikací a také informace o výsledcích zpracování těchto hrozeb.

Integrace EDR (KATA) a NDR (KATA) se konfiguruje v konzole aplikace Kaspersky Security Center. Integrovaný agent je pak spravován pomocí konzoly Kaspersky Anti Targeted Attack Platform, včetně spouštění úloh, správy objektů v karanténě, prohlížení zpráv a dalších akcí.

Konfigurace aplikace Kaspersky Endpoint Security pro fungování s EDR/NDR (KATA)

Pro fungování s EDR/NDR (KATA) lze použít následující konfigurace:

- **[KES+integrovaný agent]**. V této konfiguraci se Kaspersky Endpoint Security chová jako aplikace, která zajišťuje zabezpečení počítače, i jako aplikace pro fungování s EDR/NDR (KATA). Integrovaný agent pro EDR (KATA) je k dispozici v aplikaci Kaspersky Endpoint Security pro systém Windows 12.1 nebo novější. Integrovaný agent pro NDR (KATA) je k dispozici v aplikaci Kaspersky Endpoint Security pro systém Windows 12.7 nebo novější.
- **[EPP třetí strany+EDR Agent]**. V této konfiguraci je zabezpečení IT infrastruktury zajištěno platformou Endpoint Protection Platform (EPP) třetí strany. Interakci s EDR/NDR (KATA) zajišťuje Kaspersky Endpoint Security v konfiguraci Endpoint Detection and Response Agent (EDR Agent). V této konfiguraci je EDR Agent kompatibilní s aplikacemi EPP třetích stran. EDR Agent pro EDR (KATA) je k dispozici v aplikaci Kaspersky Endpoint Security 12.3 pro systém Windows nebo novější. EDR Agent pro NDR (KATA) je k dispozici v aplikaci Kaspersky Endpoint Security 12.7 pro systém Windows nebo novější.

Podpora pro předchozí verze Kaspersky Endpoint Security

Pokud používáte Kaspersky Endpoint Security 11.2.0–11.8.0 pro interoperabilitu s řešením Kaspersky Anti Targeted Attack Platform (EDR), součástí aplikace je Kaspersky Endpoint Agent. Aplikaci Kaspersky Endpoint Agent můžete nainstalovat, i když už v počítači je Kaspersky Endpoint Security.

Pokud používáte Kaspersky Endpoint Security 11.9.0 – 12.0, musíte aplikaci Kaspersky Endpoint Agent nainstalovat samostatně, protože počínaje verzí Kaspersky Endpoint Security 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady Kaspersky Endpoint Security.

Integrace integrovaného agenta s EDR/NDR (KATA)

Pro integraci s EDR/NDR (KATA) musíte přidat příslušnou součást: Endpoint Detection and Response (KATA) nebo Network Detection and Response (KATA). Součásti pro integraci KUMA s EDR/NDR (KATA) můžete vybrat během instalace nebo upgradu aplikace a dále použitím úlohy *Změna součástí aplikace*.

Počínaje verzí 12.11 aplikace Kaspersky Endpoint Security pro systém Windows je součást EDR (KATA) přejmenována na **Endpoint Detection and Response Expert (version 8.0 or later)**. V této verzi aplikace je součást kompatibilní s Kaspersky Anti Targeted Attack Platform 7.1 a dřívějšími verzemi a také s řešením Kaspersky Endpoint Detection and Response Expert (on-premise).

Součásti EDR Optimum, EDR Expert a EDR (KATA) nejsou vzájemně kompatibilní.

Abyste mohli EDR/NDR (KATA) používat, musí být splněny následující podmínky:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform verze 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform verze 7.0 nebo novější.
- EDR (KATA): Kaspersky Endpoint Security pro systém Windows 12.1 nebo novější. Další informace o kompatibilitě KATA s různými verzemi aplikace Kaspersky Endpoint Security najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security pro systém Windows 12.7 nebo novější.
- Kaspersky Security Center verze 14.2 nebo novější. Ve starších verzích aplikace Kaspersky Security Center není možné funkci EDR/NDR (KATA) aktivovat.

- Je aktivována aplikace a na její funkčnost se vztahuje licence.
- Jsou povoleny součásti Endpoint Detection and Response (KATA) a Network Detection and Response (KATA).
- Součásti aplikace, které zajišťují provoz EDR/NDR (KATA), jsou povoleny a funkční. Provoz EDR/NDR (KATA) zajišťují následující součásti:
  - Ochrana před souborovými hrozbami.
  - Ochrana před webovými hrozbami.
  - Ochrana před hrozbami v poště.
  - Prevence zneužití.
  - Detekce chování.
  - Prevence narušení hostitele.
  - Ochrana AMSI.
  - Kontrola na pozadí.
  - Kaspersky Security Network.

Integrace s řešením Endpoint Detection and Response (KATA) sestává z následujících kroků:

1. **Instalace součástí Endpoint Detection and Response (KATA) a Network Detection and Response (KATA)**

   Součásti EDR (KATA) a NDR (KATA) můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

   Pro dokončení aktualizace aplikace novými součástmi je nutné restartovat počítač.

2 **Aktivace řešení Network Detection and Response (KATA) a Endpoint Detection and Response (KATA)**

Musíte si koupit samostatnou licenci pro EDR (KATA) a NDR (KATA) (například doplněk součásti Kaspersky Endpoint Detection and Response (KATA)).

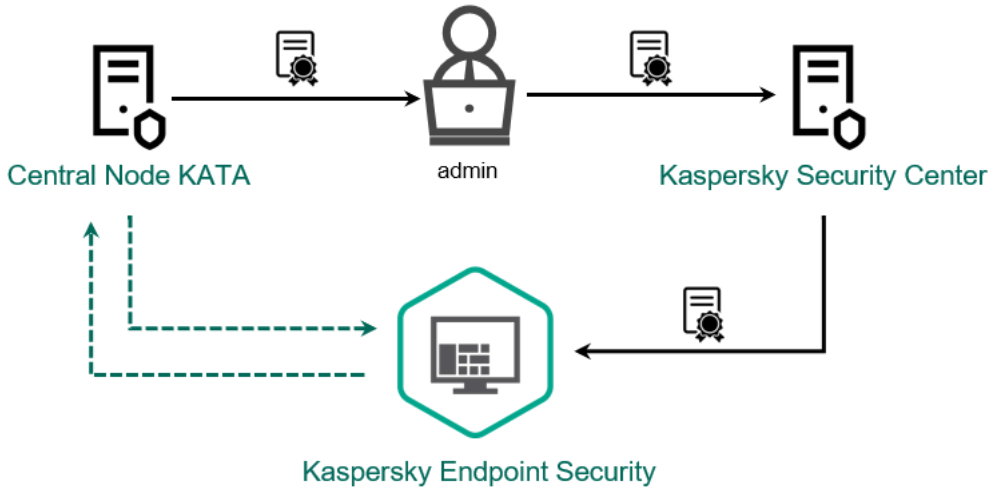
Funkce bude dostupná po přidání samostatného klíče, který pokrývá funkce EDR (KATA) a NDR (KATA). V počítači tak je přidáno více klíčů: klíč pro aplikaci Kaspersky Endpoint Security a klíče pro řešení Kaspersky Endpoint Detection and Response (KATA) a Network Detection and Response (KATA).

Fungování licence k samostatné funkci EDr (KATA) a NDR (KATA) je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

Ověřte, zda jsou obě funkce EDR (KATA) a NDR (KATA) součástí licence a jsou spuštěny v místním rozhraní aplikace.

3 **Připojení k součásti Central Node**

Součást Kaspersky Anti Targeted Attack Platform vyžaduje vytvoření důvěryhodného spojení mezi aplikací Kaspersky Endpoint Security a součástí Central Node. Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).



Přidání certifikátu TLS do aplikace Kaspersky Endpoint Security

Ve výchozím nastavení Kaspersky Endpoint Security kontroluje pouze certifikát TLS součásti Central Node. Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače na součásti Central Node (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení součásti Central Node a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte možnost **Detection and Response** a vyberte součást, kterou chcete nakonfigurovat: **Endpoint Detection and Response Expert (on-premise)** nebo **Network Detection and Response (KATA)**.
5. Zaškrtněte příslušné zaškrtávací políčko: **Endpoint Detection and Response Expert (verze 7.1 nebo starší)** nebo **Network Detection and Response (KATA)**.
6. Klikněte na tlačítko **Nastavení připojení k serveru**.
7. Nakonfigurujte připojení k serveru:
   - **Doba vypršení časového limitu (s)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Certifikát TLS serveru**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
   - **Používat ověřování na obou stranách**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

8. Klikněte na tlačítko **OK**.
9. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

   Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
10. V případě potřeby nakonfigurujte telemetrii.
11. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak připojit počítač Kaspersky Endpoint Security k součásti Central Node pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **Built-in Agents Configuration** a vyberte součást, kterou chcete konfigurovat: **Endpoint Detection and Response Expert (on-premise)** nebo **Network Detection and Response (KATA)**.
5. Zapněte příslušný přepínač: **Endpoint Detection and Response Expert (on-premise) ENABLED** nebo **Network Detection and Response (KATA) ENABLED**.
6. Chcete-li nakonfigurovat EDR (KATA), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
7. Klikněte na tlačítko **Connection settings**.
8. Nakonfigurujte připojení k serveru:
   - **Timeout (sec)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
   - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
   - **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.
9. Klikněte na tlačítko **OK**.
10. Přidejte servery součásti Central Node. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

    Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.
11. V případě potřeby nakonfigurujte telemetrii.
12. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Certifikát TLS můžete také přidat lokálně pomocí příkazového řádku.

Počítač je tak přidán do konzoly součásti Kaspersky Anti Targeted Attack Platform. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součástí můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součásti **Endpoint Detection and Response Expert (version 8.0 or later)** a **Network Detection and Response (KATA)** budou přidány na seznam součástí aplikace Kaspersky Endpoint Security.

Stav součástí v konzole aplikace Kaspersky Security Center můžete zjistit ve vlastnostech počítače v oddílu **Components**. Při kontrole stavu součásti v konzole zvažte následující skutečnosti. Pokud součást není nainstalována a na funkce se nevztahuje vaše licence, v konzole se zobrazí stav **Not supported by license** místo **Not installed**.

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro systém Windows můžete sledovat stav součásti EDR (KATA) v konzole pro správu aplikace Kaspersky Security Center (MMC). Aktuální stav součásti se zobrazuje ve vlastnostech počítače ve sloupci **Endpoint Sensor status** (*Running*, *Starting*, *Stopped*, *Paused*, *Failed*, *Unknown*). Webová konzola nezobrazuje stav nástroje Endpoint Sensor.

Konfigurace telemetrie EDR (KATA)

Telemetrie je seznam událostí, ke kterým došlo na chráněném počítači. Kaspersky Endpoint Security analyzuje telemetrická data a během synchronizace je odesílá do součásti Kaspersky Anti Targeted Attack Platform. Telemetrické události přicházejí na server téměř nepřetržitě. Kaspersky Endpoint Security zahájí synchronizaci se serverem, když je splněna některá z následujících podmínek:

- Interval synchronizace vypršel.
- Počet událostí ve vyrovnávací paměti překročí horní limit.

Ve výchozím nastavení se tedy aplikace synchronizuje každých 30 sekund nebo vždy, když vyrovnávací paměť obsahuje 1024 událostí. Chování synchronizace můžete nakonfigurovat v zásadách aplikace Kaspersky Endpoint Security a vybrat optimální hodnoty, aby odpovídaly zatížení vaší sítě (viz pokyny níže).

Pokud mezi aplikací Kaspersky Endpoint Security a serverem není navázáno připojení, aplikace zařadí nové události do fronty. Po obnovení připojení odešle Kaspersky Endpoint Security události ve frontě na server ve správném pořadí. Aby nedošlo k přetížení serveru, může aplikace Kaspersky Endpoint Security některé události přeskočit. Chcete-li to povolit, můžete optimalizovat nastavení přenosu událostí, například nastavit maximální hodnotu událostí za hodinu (viz pokyny níže).

Pokud používáte Kaspersky Anti Targeted Attack Platform spolu s jiným řešením, které také využívá telemetrii, můžete telemetrii pro KATA (EDR) vypnout (viz pokyny níže). To vám umožní optimalizovat zatížení serveru pro tato řešení. Pokud máte například nasazené řešení Managed Detection and Response a součást KATA (EDR), můžete použít telemetrii MDR a vytvářet úlohy Reakce na hrozby v KATA (EDR).

Jak konfigurovat telemetrii v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte možnost **Detection and Response** a vyberte součást, kterou chcete nakonfigurovat: **Endpoint Detection and Response Expert (on-premise)** nebo **Network Detection and Response (KATA)**.
5. Nakonfigurujte nastavení **Odesílat požadavek na synchronizaci na server KATA každých (min.)**. Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.
6. Ujistěte se, že je zaškrtnuto políčko **Odesílat telemetrické údaje do KATA**.
7. V případě potřeby nakonfigurujte synchronizaci s nastavením serveru v bloku **Nastavení přenosu dat**:
   - **Maximální prodleva přenosu událostí (sek.)**. Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
   - **Maximální počet balíčků událostí**. Aplikace se synchronizuje se serverem, když se vyrovnávací paměť zaplní událostmi. Výchozí hodnota je 1024 událostí.
8. V případě potřeby zaškrtněte políčko **Povolit omezování požadavků** v bloku **Omezování požadavků**.

   Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.
9. Konfigurace nastavení optimalizace pro odesílání událostí na server:
   - **Maximální počet událostí za hodinu**. Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
   - **Procentní hodnota překročení limitu událostí**. Aplikace třídí události podle typu (například události „změny registru") a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.

10. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak konfigurovat telemetrii ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premise)**.
5. Chcete-li nakonfigurovat EDR (KATA), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 7.1 or earlier)**.
6. Ujistěte se, že je v bloku **Data transmission settings** zaškrtnuto políčko **Send telemetry to KATA servers**.
7. Nakonfigurujte nastavení **Send sync request to server every (min)**. Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.
8. Ujistěte se, že je zaškrtnuto políčko **Send telemetry to KATA servers**.
9. V případě potřeby nakonfigurujte synchronizaci s nastavením serveru v bloku **Data transmission settings**:
   - **Maximum event transmission delay (sec)**. Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
   - **Maximum number of event packages**. Aplikace se synchronizuje se serverem, když se vyrovnávací paměť zaplní událostmi. Výchozí hodnota je 1024 událostí.
10. V případě potřeby zaškrtněte políčko **Enable request throttling** v bloku **Request throttling**.

    Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.
11. Konfigurace nastavení optimalizace pro odesílání událostí na server:
    - **Maximum number of events per hour**. Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
    - **Percentage of event limit excess**. Aplikace třídí události podle typu (například události „změny registru") a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.
12. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte do části **Integrace KATA** → **Výjimky telemetrie**.
5. V části **Nastavení přenosu dat** zaškrtněte políčko **Použít výjimky**.
6. Klikněte na možnost **Přidat** a nakonfigurujte výjimky:

   Kritéria lze spojovat pomocí logického *AND*.

   - **Cesta**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Aby výjimka fungovala, musí být zadána cesta k souboru.

- **Příkazový řádek**. Příkaz používaný ke spuštění objektu.
- **Popis**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
  Podrobnější informace prostředku VersionInfo najdete na webu společnosti Microsoft.
- **Původní název souboru**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Verze**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **MD5**. Hodnota hash MD5 souboru.
- **SHA256**. Hodnota hash SHA256 souboru.
- **Typ události**. Aby výjimka fungovala, musíte vybrat alespoň jeden typ události.

7. Uložte změny.

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Tasks**.
   Otevře se seznam úloh.
2. Klikněte na tlačítko **New task**.

Spustí se průvodce úlohou. Postupujte podle pokynů průvodce.

Krok 1. Volba typu úlohy

1. Vyberte možnost **Kaspersky Endpoint Security pro systém Windows (14.0) → Vrácení aktualizace zpět**.

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 úloh, například ručně.

Krok 4. Definování názvu úlohy

Zadejte název úlohy.

Krok 7. Dokončení vytvoření úlohy

Ukončete průvodce. V případě potřeby zaškrtněte políčko **Run the task after the wizard finishes**. Průběh úlohy můžete sledovat ve vlastnostech úlohy.

Výjimky z telemetrie EDR (KATA)

Chcete-li zlepšit výkon a optimalizovat přenos dat na telemetrický server, můžete nakonfigurovat výjimky z telemetrie. Můžete se například rozhodnout neposílat data o síťové komunikaci u jednotlivých aplikací.

Jak vytvořit výjimku z telemetrie v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
4. V bloku **Nastavení telemetrie** → **Telemetrie EDR (KATA) / NDR (KATA)** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, nakonfigurujte výjimky z telemetrie (viz tabulka níže).

   Aplikace kombinuje podmínky výjimky logickým AND. Chcete-li vytvořit pravidlo, musíte zadat hodnotu v poli **Úplná cesta** a v seznamu **Použít u následujících typů událostí** vybrat v poli alespoň jeden typ události.
6. Uložte změny.

[Jak vytvořit výjimku z telemetrie ve webové konzole a cloudové konzole]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Telemetry Settings**.
5. Vyberte kartu **EDR (KATA) / NDR (KATA) telemetry**.
6. V okně, které se otevře, nakonfigurujte výjimky z telemetrie (viz tabulka níže).

   Aplikace kombinuje podmínky výjimky logickým AND. Chcete-li vytvořit pravidlo, musíte zadat hodnotu v poli **Full path** a vybrat alespoň jeden typ události.
7. Uložte změny.

Parametry výjimek z telemetrie

Parametr	Popis
Vyloučené procesy	**Optimalizovat velikost odesílané telemetrie**. Kaspersky Endpoint Security umožňuje optimalizovat množství přenášených dat a vyloučit z telemetrie události s určitými kódy: kód 102 (základní komunikace) a 8 (síťová aktivita procesu) pro protokol Microsoft SMB, službu WinRM a proces klnagent.exe součásti Network Agent, stejně jako rozšířené informace o typech síťových paketů pro všechny typy síťových protokolů. Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO. **Process** a **Parent process**: • **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. • **Command line text**. Příkaz používaný ke spuštění souboru. • **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo). • **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo). • **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo). • **File checksums**. MD5 a SHA256. Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru. V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému. **Použít u následujících typů událostí**: • **Změna souboru**. • **Události sítě**. • **Proces: interaktivní vstup v konzole**. • **Modul byl načten**. • **Byl změněn registr**.

- **Protokoly DNS**.
- **Přístup k procesům**.
- **Vložení kódu**.
- **Dotaz WMI**.
- **Kanál**.
- **LDAP**.
- **AMSI**.

Vyloučená síťová komunikace

Název pravidla.

Směr.

Protokol.

Základní soket.

Číslo protokolu.

Certifikát TLS.

Místní port nebo rozsah.

Vzdálený port nebo rozsah.

Místní adresa. Síťová adresa počítače, u kterého aplikace Kaspersky Endpoint Security vylučuje telemetrii ze síťového provozu.

Vzdálená adresa. Síťová adresa počítače, u kterého aplikace Kaspersky Endpoint Security vylučuje telemetrii ze síťového provozu.

Pro adresy IP je podporován pouze formát IPv4.

Aplikace. Seznam spustitelných souborů aplikací, u kterých Kaspersky Endpoint Security vylučuje telemetrii EDR ze síťového provozu.

Vyloučené operace se souborem

Název pravidla.

Název souboru nebo maska. Název nebo maska souboru nebo složky; Kaspersky Endpoint Security použije při přístupu k tomuto souboru nebo složce pravidlo výjimky. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`.

Typ operace.

Předchozí cesta.

> Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.
- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

> V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené operace DNS

Název pravidla.

> Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.

- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

DNS:

- **IP adresa serveru DNS**.
- **Možnosti dotazu**.
- **Stav**.
- **Název domény**.
- **ID typu nastavení**.
- **Data odpovědi**.

Vyloučené operace LDAP

Název pravidla.

Rozsah vyhledávání LDAP.

Filtr.

Rozlišující název pro vyhledávání objektů LDAP.

Atributy objektu.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.
- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené dotazy na přístup k procesům

Název pravidla.

Typ operace.

Přístup vyžádaný procesem.

Trasování zásobníku volání.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process, **Parent process**, **File of a target process**, **Handle to the source process** a **Handle to the target process**.

- **Úplná cesta**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Text příkazového řádku**. Příkaz používaný ke spuštění souboru.

- **Zadejte kritéria pro aktivaci pravidla a typy událostí, u kterých se má toto pravidlo použít**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Původní název souboru**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Verze**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **Kontrolní součty souborů**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené injektáže kódu

Název pravidla.

Způsob přístupu.

Zásobník volání.

Upravený příkazový řádek.

Adresa injektáže.

Název vloženého DLL.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.
- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené dotazy WMI

Název pravidla.

Typ operace WMI.

Vzdálený dotaz.

Název počítače, který provedl příkaz WMI.

Uživatelský účet WMI.

Provedený příkaz WMI.

Obor názvů WMI.

Filtr konzumentů událostí WMI.

Název vytvořeného konzumenta událostí WMI.

Zdrojový kód konzumenta událostí WMI.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.

- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené operace kanálu

Název pravidla.

Název kanálu.

Typ operace.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.
- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené změny registru

Název pravidla.

Typ operace.

Cesta.

Název hodnoty.

Hodnota.

Úplný název souboru registru.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Process a **Parent process**:

- **Full path**. Úplná cesta k souboru včetně jeho názvu a přípony. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`.
- **Command line text**. Příkaz používaný ke spuštění souboru.
- **Description**. Hodnota parametru FileDescription z prostředku RT_VERSION (VersionInfo).
- **Original file name**. Hodnota parametru OriginalFilename z prostředku RT_VERSION (VersionInfo).
- **Version**. Hodnota parametru FileVersion z prostředku RT_VERSION (VersionInfo).
- **File checksums**. MD5 a SHA256.

Soubor můžete vybrat také ručně a aplikace automaticky vyplní pole z vybraného souboru.

V 64bitových operačních systémech musíte ručně zadat parametry 64bitové verze spustitelného souboru procesu ze složky `C:\windows\system32`, protože aplikace vyplní pole parametrů spustitelného souboru daty z vlastností 32bitové verzi stejného spustitelného souboru ve složce `C:\windows\syswow64`. Pokud například vyberete `C:\windows\system32\cmd.exe`, modul plug-in zobrazí parametry `C:\windows\syswow64\cmd.exe`. Toto chování je dáno zvláštnostmi operačního systému.

Vyloučené operace se zařízeními

Název pravidla.

Typ zařízení.

ID zařízení.

Název zařízení.

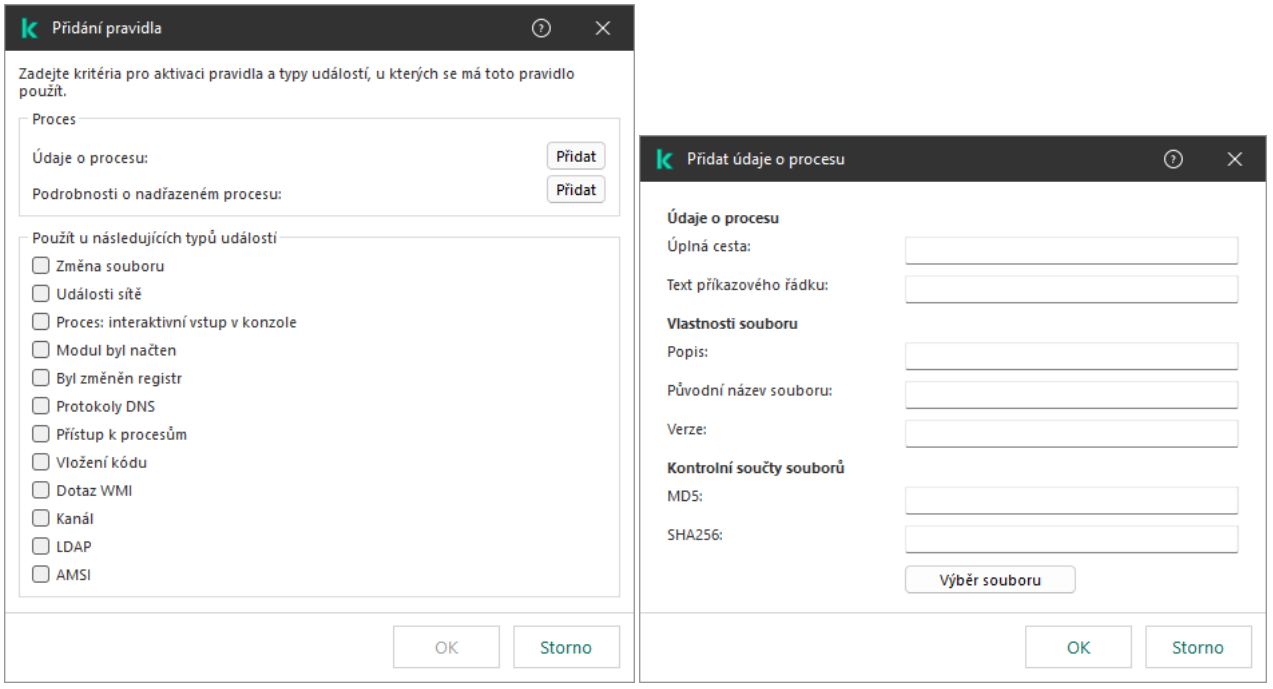
Příklad 1. Vyloučené procesy

Chcete-li z telemetrie vyloučit události aplikace (procesu) třetí strany, otevřete okno výjimek z telemetrie EDR na kartě **Vyloučené procesy** a přidejte spustitelný soubor aplikace.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Příklad:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Vyloučení procesu

Příklad 1. Změna souboru

Pokud často upravujete skripty v aplikaci Notepad++ a chcete vyloučit události úpravy pro příslušné skripty, přidejte do výjimek z telemetrie spustitelný soubor Notepad++.

Zadejte nastavení takto:

- **Úplná cesta**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **Použít u následujících typů událostí**: Změna souboru.

Příklad 2. Události sítě

Pokud používáte pro správu souborů na vzdáleném serveru aplikaci WinSCP aplikaci a chcete vyloučit síťové události, přidejte do výjimek z telemetrie spustitelný souboru aplikace WinSCP.

Zadejte nastavení takto:

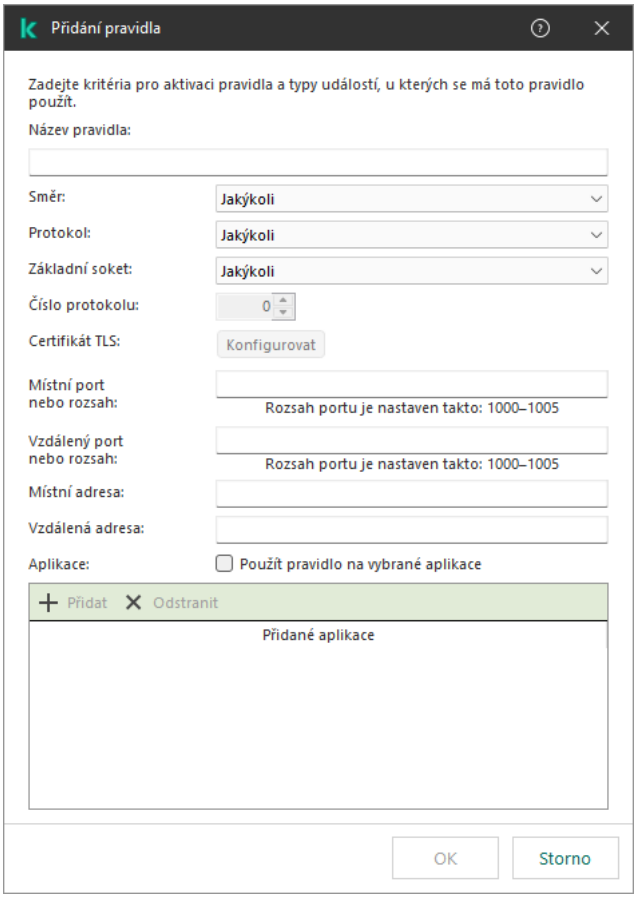
- **Úplná cesta**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (volitelné).
- **Použít u následujících typů událostí**: Události sítě.

Příklad 2. Vyloučená síťová komunikace

Chcete-li z telemetrie vyloučit události připojení ke vzdálené službě, otevřete okno výjimek z telemetrie EDR na kartě **Vyloučená síťová komunikace** a přidejte nastavení připojení: protokol, port, směr, IP adresa, certifikát TLS a další.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Nelze zadat adresu podsítě (například 10.28.0.0/24). Aplikace umožňuje zadat pouze jednu IP adresu (například 10.28.0.105).



Výjimka ze síťové komunikace

Pokud používáte podnikový webový server a chcete při připojování k tomuto webovému serveru vyloučit události prohlížeče, přidejte do výjimek z telemetrie IP adresu serveru a spustitelný soubor prohlížeče.

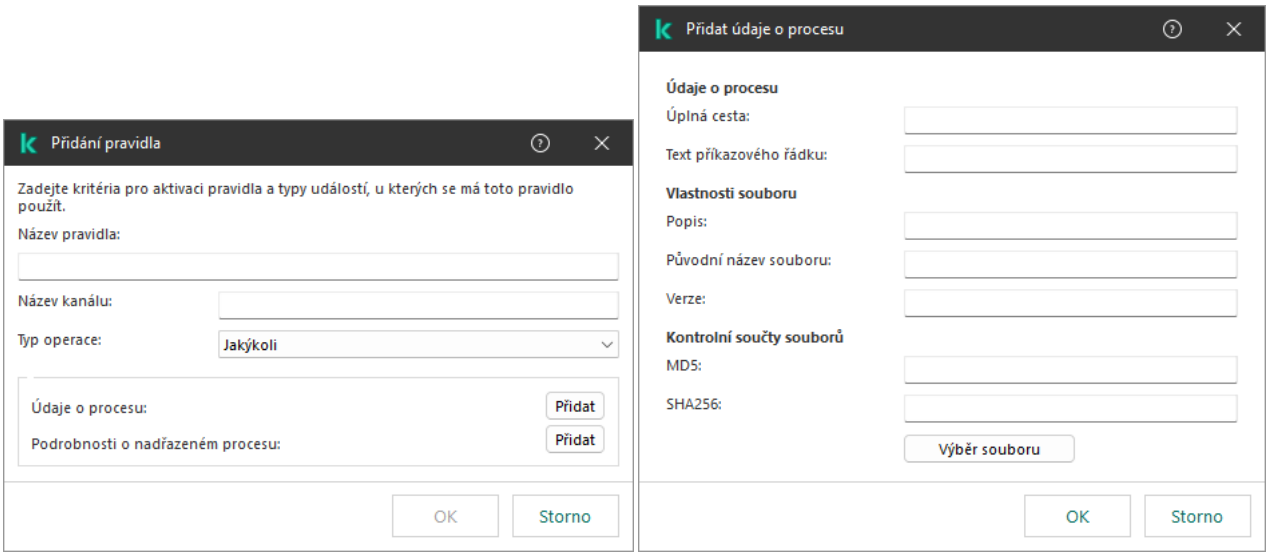
Zadejte nastavení takto:

- **Protokol**: TCP.
- **Vzdálený port nebo rozsah**: 443.
- **Vzdálená adresa**: 10.28.0.105.
- **Aplikace**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

Příklad 3. Vyloučené operace se souborem

Chcete-li z telemetrie vyloučit události zahrnující operace s důvěryhodnými soubory, otevřete okno výjimek z telemetrie EDR na kartě **Vyloučené operace se souborem** a přidejte důvěryhodný soubor.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.



Vyloučené operace se souborem

Pokud aplikace zapisuje do protokolu a vy chcete vyloučit události úpravy souboru protokolu, přidejte do výjimek z telemetrie soubor protokolu a spustitelný soubor aplikace.

Zadejte nastavení takto:

- **Název souboru nebo maska**: `C:\Apache24\logs\error.log`.
- **Typ operace**: Změna souboru.
- **Úplná cesta**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

Příklad 4. Vyloučené změny registru

Chcete-li z telemetrie vyloučit události úpravy registru, otevřete okno výjimek z telemetrie EDR na kartě **Vyloučené změny registru** a přidejte klíč registru.

Kaspersky Endpoint Security kombinuje kritéria aktivující pravidlo logickým ANO.

Pokud aplikace často upravuje hodnoty registru a vy chcete tyto události úpravy registru vyloučit z telemetrie, přidejte do výjimek z telemetrie klíč registru a spustitelný soubor aplikace.

Zadejte nastavení takto:

- **Typ operace**: Upravit.
- **Cesta**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.
- **Úplná cesta**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

Kaspersky Anti Targeted Attack Platform zahrnuje součást Sandbox (KATA Sandbox). *Sandbox* je technologie, která vám umožňuje v počítači detekovat pokročilé hrozby. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Podrobnosti o tomto řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

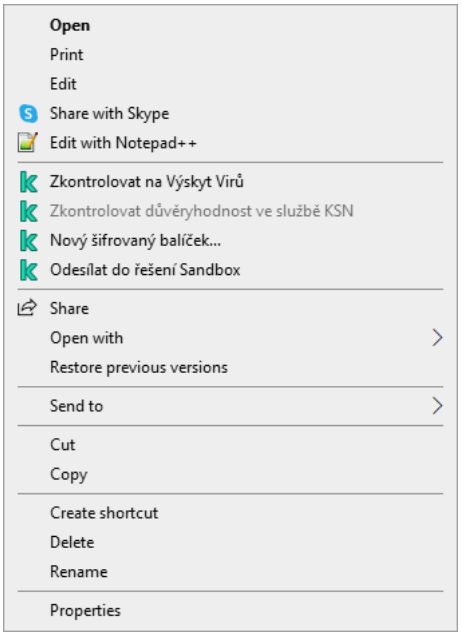
Chcete-li aktivovat součást KATA Sandbox, potřebujete licenční klíč, který zahrnuje funkci KATA nebo KEDR. Podrobnosti o dostupných funkcích najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

KATA Sandbox umožňuje kontrolu souborů v následujících režimech:

- *Ručně.* Uživatel ručně odešle soubor ke kontrole z kontextové nabídky (**Odesílat do řešení Sandbox**). Při odeslání souboru do součásti Sandbox aplikace zkontroluje soubor pomocí antivirových databází.
- *Automaticky.* Aplikace automaticky detekuje objekty a odesílá je do součásti Sandbox ke kontrole.

Po odeslání souboru do součásti Sandbox zůstane soubor přístupný uživateli. Kaspersky Endpoint Security zaznamená odpovídající událost do protokolu a odešle událost do aplikace Kaspersky Security Center a konzoly Kaspersky Anti Targeted Attack Platform. Pokud Sandbox zjistí škodlivou aktivitu, Kaspersky Endpoint Security automaticky provede akci součásti Reakce na hrozbu (například odstraní objekt a zahájí kontrolu kritických oblastí).

Aby součást KATA Sandbox fungovala v ručním režimu, musí být nasazena platforma Kaspersky Anti Targeted Attack Platform 7.0 nebo novější. Aby součást KATA Sandbox fungovala v automatickém režimu, musí být nasazena platforma Kaspersky Anti Targeted Attack Platform 8.0 nebo novější.



Kontrola v součásti KATA Sandbox z místní nabídky

Integrace integrovaného agenta s řešením KATA Sandbox

Pro integraci s řešením KATA Sandbox je vyžadováno přidání součásti Sandbox. Součást Sandbox můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

Chcete-li odeslat soubory ke kontrole, musíte povolit integraci se součástí KATA Sandbox a přidat server Central Node, který je nasazen v rámci řešení. Součást lze spravovat pouze pomocí webové konzoly Kaspersky Security Center. Tuto součást nemůžete spravovat pomocí konzoly pro správu (MMC).

Postup povolení nebo zakázání integrace s řešením KATA Sandbox:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Sandbox**.
5. Pomocí přepínače **Integration with Sandbox ENABLED** můžete tuto součást povolit nebo zakázat.
6. Vyberte provozní režim Sandbox KATA:
   - **Manually**. Uživatel ručně odešle soubor ke kontrole z kontextové nabídky (**Odesílat do řešení Sandbox**).
   - **Automatically**. Aplikace automaticky detekuje objekty a odesílá je do součásti Sandbox ke kontrole.
   - **Combined**.
7. Klikněte na odkaz **Connection settings**.
8. Konfigurace nastavení připojení k serveru součásti Central Node:
   - **Timeout (msec)**. Časový limit připojení pro server Central Node. Po uplynutí nastaveného časového limitu odešle aplikace Kaspersky Endpoint Security požadavek na další server. Pokud je rychlost připojení nízká nebo je připojení nestabilní, můžete prodloužit časový limit připojení pro server. Doporučovaný časový limit požadavku je 0,5 sekundy a méně.
   - **Request queue**. Velikost složky fronty žádostí. Při odesílání více objektů ke kontrole v součásti Sandbox vytvoří Kaspersky Endpoint Security frontu požadavků. Ve výchozím nastavení je velikost složky fronty žádostí omezena na 100 MB. Jakmile je dosaženo maximální velikosti, Sandbox

přestane přidávat nové žádosti do fronty a odešle odpovídající událost do aplikace Kaspersky Security Center. Velikost složky fronty žádostí můžete konfigurovat v závislosti na konfiguraci serveru.

- **Server TLS certificate**. Chcete-li konfigurovat důvěryhodné připojení k serverům Central Node, musíte si připravit certifikát TLS. Poté musíte přidat certifikát do počítače pomocí zásady. Musíte také přidat certifikát na server Central Node.

- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

9. V bloku **Connection to Sandbox servers** klikněte na tlačítko **Add**.

10. Otevře se okno; v okně zadejte adresu a port serveru Central Node (IPv4, IPv6, DNS).

    Podrobnosti o nasazení virtuálních bitových kopií a konfiguraci serverů Central Node najdete v nápovědě k řešení Kaspersky Anti Targeted Attack Platform .

11. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Součást Sandbox je tak povolena. Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Sandbox** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Konfigurace akcí součásti Reakce na hrozbu

Pokud Sandbox zjistí škodlivou aktivitu, Kaspersky Endpoint Security automaticky provede akci součásti Reakce na hrozbu (například odstraní objekt a zahájí kontrolu kritických oblastí).

Postup konfigurace akcí součásti Reakce na hrozby:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Built-in Agents Configuration** → **Sandbox**.

5. V části **Action on threat detection** vyberte příslušnou akci:

   - **Move copy to Quarantine, delete object**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security odstraní škodlivý objekt nalezený v počítači. Před odstraněním objektu vytvoří aplikace Kaspersky Endpoint Security záložní kopii pro případ, že bude nutné objekt později obnovit. Kaspersky Endpoint Security přesune záložní kopii do karantény.

   - **Run Critical Areas Scan**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security spustí úlohu *Kontrola kritických oblastí*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků.

   - **Create IOC Scan task**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security automaticky vytvoří úlohu *Kontrola IOC (autonomní úloha kontroly IOC)*. Pro tuto úlohu můžete nakonfigurovat režim spuštění, rozsah kontroly a akci při detekci IOC: odstranit objekt, spustit úlohu *Kontrola kritických oblastí*. Chcete-li upravit další nastavení úlohy *Kontrola IOC*, přejděte do nastavení úlohy.

6. V případě potřeby nakonfigurujte nastavení úlohy *Kontrola IOC* v bloku **IOC Scan scope**.

   - **Critical file areas**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security provede kontrolu IOC pouze v kritických oblastech souboru počítače: paměti jádra a spouštěcí sektory.

   - **File areas on system drives of the computer**. Je-li vybrána tato možnost, provede Kaspersky Endpoint Security kontrolu IOC na systémové jednotce počítače.

7. V případě potřeby nakonfigurujte nastavení úlohy *Kontrola IOC* v bloku **Run IOC Scan task**.

   - **Manually**. Režim spuštění, ve kterém můžete úlohu *Kontrola IOC* spustit ručně v době, kdy je to pro vás výhodné.

   - **Automatically**. Režim spuštění, ve kterém aplikace Kaspersky Endpoint Security spouští úlohu *Kontrola IOC* automaticky, kdykoli je detekována hrozba.

   - **Run only when the computer is idle**. Režim spuštění, ve kterém aplikace Kaspersky Endpoint Security spouští úlohu *Kontrola IOC*, když je aktivní spořič obrazovky nebo je obrazovka zamčená. Pokud uživatel odemkne počítač, aplikace Kaspersky Endpoint Security úlohu pozastaví. To znamená, že dokončení úlohy může trvat několik dní.

8. Nakonfigurujte pokročilá nastavení úlohy pro úlohu *Kontrola IOC*.

9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Průvodce migrací KEA na KES pro EDR (KATA)

Počínaje verzí 12.1 aplikace Kaspersky Endpoint Security pro systém Windows obsahuje integrovaného agenta pro správu součásti Kaspersky Endpoint Detection and Response jako součásti řešení Kaspersky Anti Targeted Attack Platform. Pro práci s řešením EDR (KATA) už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent. Všechny funkce aplikace Kaspersky Endpoint Agent bude provádět aplikace Kaspersky Endpoint Security. Zatížení serverů Kaspersky Anti Targeted Attack Platform zůstane stejné.

Když nasadíte Kaspersky Endpoint Security do počítačů s nainstalovanou aplikací Kaspersky Endpoint Agent, řešení Kaspersky Anti Targeted Attack Platform (EDR) bude nadále fungovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent. Ke stejnému chování v systému dojde, když aktualizujete Kaspersky Endpoint Security na verzi 12.1 a novější.

Aplikace Kaspersky Endpoint Security není kompatibilní s aplikací Kaspersky Endpoint Agent. Obě tyto aplikace nelze nainstalovat do stejného počítače.

Aby aplikace Kaspersky Endpoint Security fungovala jako součást řešení Endpoint Detection and Response (KATA), musí být splněny následující podmínky:

- Kaspersky Anti Targeted Attack Platform verze 5.0 nebo novější.
- Kaspersky Security Center verze 14.2 nebo vyšší (včetně součásti Network Agent). Ve starších verzích aplikace Kaspersky Security Center není možné funkci Endpoint Detection and Response (KATA) aktivovat.

Kroky pro migraci konfigurace [KES+KEA] na [KES+integrovaný agent] pro EDR (KATA)

1. **Upgrade modulu plug-in pro správu aplikace Kaspersky Endpoint Security**

   Součást EDR (KATA) lze spravovat pomocí modulu plug-in pro správu aplikace Kaspersky Endpoint Security verze 12.1 nebo novější. V závislosti na typu konzoly aplikace Kaspersky Security Center, kterou používáte, aktualizujte modul plug-in pro správu v konzole pro správu (MMC) nebo webový modul plug-in ve webové konzole.

2. **Migrace zásady a úloh**

   Nastavení aplikace Kaspersky Endpoint Agent můžete přenést do aplikace Kaspersky Endpoint Security pro Windows. K dispozici jsou následující možnosti:

   - Průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security. Průvodce migrací z aplikace Kaspersky Endpoint Agent na aplikaci Kaspersky Endpoint Security funguje pouze ve webové konzole.

     Jak migrovat nastavení zásad a úloh z aplikace Kaspersky Endpoint Agent do aplikace Kaspersky Endpoint Security ve webové konzole

     V hlavním okně webové konzoly vyberte možnosti **Operations → Migration from Kaspersky Endpoint Agent**.

     Tím spustíte průvodce migrací zásad a úloh. Postupujte podle pokynů průvodce.

     #### Krok 1. Migrace zásad

     Průvodce migrací vytvoří novou zásadu, která sloučí nastavení zásad aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. V seznamu zásad vyberte zásady aplikace Kaspersky Endpoint Agent, jejichž nastavení chcete sloučit se zásadami aplikace Kaspersky Endpoint Security. Kliknutím na zásadu aplikace Kaspersky Endpoint Agent vyberte zásadu aplikace Kaspersky Endpoint Security, s níž chcete sloučit nastavení. Zkontrolujte, zda jste vybrali správné zásady, a přejděte k dalšímu kroku.

     #### Krok 2. Migrace úloh

     Průvodce migrací nepodporuje úlohy EDR (KATA). Tento krok přeskočte.

     #### Krok 3. Dokončení průvodce

     Ukončete průvodce. Bude vytvořena nová zásada aplikace Kaspersky Endpoint Security. V zásadě se sloučí nastavení z aplikací Kaspersky Endpoint Security a Kaspersky Endpoint Agent. Název zásady je *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Nová zásada má stav *Inactive*. Chcete-li pokračovat, změňte stav zásad aplikací Kaspersky Endpoint Agent a Kaspersky Endpoint Security na *Inactive* a aktivujte novou sloučenou zásadu.

     Průvodce migrací ve webové konzole přeskočí následující nastavení zásad a nemigruje je:

     - Zákaz změny nastavení **Connection settings** („zámek").

       Ve výchozím nastavení lze nastavení měnit („zámek" je otevřený). Nastavení se proto v počítači nepoužijí. Musíte zakázat změnu nastavení a „zámek" zavřít.

     - Kryptokontejner.

Pokud pro připojení k serverům Central Node používáte obousměrné ověřování, musíte znovu přidat kryptokontejner.

Jelikož průvodce migrací tato nastavení nemigruje, můžete při připojování počítače k serverům centrálního uzlu narazit na chyby. Chcete-li chyby opravit, musíte přejít do vlastností zásad a nakonfigurovat nastavení připojení.

- Standardní průvodce hromadným převodem zásad a úloh. Průvodce hromadným převodem zásad a úloh je k dispozici pouze v konzole pro správu (MMC). Další podrobnosti o průvodci hromadným převodem zásad a úloh naleznete v nápovědě k aplikaci Kaspersky Security Center.

Abyste se ujistili, že aplikace Kaspersky Endpoint Security na serverech funguje správně, doporučujeme přidat soubory důležité pro fungování serveru do důvěryhodné zóny. U serverů SQL musíte přidat databázové soubory MDF a LDF. U serverů Microsoft Exchange musíte přidat soubory CHK, EDB, JRS, LOG a JSL. Můžete použít masky, např. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

Nastavení výjimek telemetrie EDR se ze zásad aplikace Kaspersky Endpoint Agent do zásad aplikace Kaspersky Endpoint Security nemigrují. Kaspersky Endpoint Security má své vlastní nástroje pro výjimky – důvěryhodné aplikace. Provoz aplikace Kaspersky Endpoint Security je optimalizován tak, aby absence individuálních výjimek telemetrie EDR nezpůsobila ve srovnání s aplikací Kaspersky Endpoint Agent žádné další zatížení vašeho počítače. Aplikace Kaspersky Endpoint Security využívá telemetrii nejen pro EDR (KATA), ale také pro provoz součástí ochrany aplikací. Není tedy potřeba přenášet jednotlivé výjimky telemetrie EDR. Pokud se výkon počítače sníží, zkontrolujte činnost aplikace (viz krok 7 Kontrola výkonu).

3 Licence k funkci EDR (KATA)

Chcete-li aktivovat Kaspersky Endpoint Security jako součást řešení Kaspersky Anti Targeted Attack Platform, potřebujete samostatnou licenci pro doplněk Kaspersky Endpoint Detection and Response (KATA). Klíč můžete přidat pomocí úlohy *Add key*. Do aplikace tak budou přidány dva klíče: *Kaspersky Endpoint Security* a *Kaspersky Endpoint Detection and Response (KATA)*.

Licence k doplňku Kaspersky Endpoint Detection and Response (KATA) na počítačích s dříve aktivovanými funkcemi EDR Optimum nebo EDR Expert zahrnuje následující zvláštní aspekty:

- Pokud používáte pro licencování aplikace Kaspersky Endpoint Security s funkcemi EDR Optimum nebo EDR Expert *soubor klíče*, nelze přidat samostatný klíč pro Kaspersky Endpoint Detection and Response (KATA). Můžete buď přejít na používání aktivačního kódu pro licencování, nebo se obrátit na poskytovatele služeb a získat nový soubor klíče pro aktivaci funkcí Kaspersky Endpoint Security a EDR. Poskytovatel služeb poskytne pro licencování jeden nebo více souborů klíče.

- Pokud používáte pro licencování aplikace Kaspersky Endpoint Security bez funkcí EDR Optimum nebo EDR Expert *soubor klíče*, můžete přidat samostatný klíč k doplňku Kaspersky Endpoint Detection and Response (KATA), aniž by bylo nutno znovu vydávat soubory klíče.

- Pokud používáte pro licencování *aktivační kód*, aktivační server Kaspersky automaticky znovu vydá klíče a funkce EDR (KATA) budou automaticky dostupné. V tomto případě budou funkce EDR Optimum a EDR Expert deaktivovány.

- Kaspersky Endpoint Security vám umožňuje přidat až dva aktivní klíče: klíč k aplikaci Kaspersky Endpoint Security a klíč typu doplňku. Můžete také přidat až dva rezervní klíče. Jeden rezervní klíč Kaspersky Endpoint Security a jeden rezervní klíč typu doplňku.

4 Instalace/upgrade aplikace Kaspersky Endpoint Security

Pro migraci funkce EDR (KATA) během instalace nebo upgradu aplikace se doporučuje použít úlohu vzdálené instalace. Při vytváření úlohy vzdálené instalace je třeba v nastavení instalačního balíčku vybrat součást EDR (KATA).

Aplikaci můžete také upgradovat následujícími způsoby:

- Pomocí aktualizační služby Kaspersky.

- Místně pomocí průvodce instalací.

Aplikace Kaspersky Endpoint Security podporuje automatický výběr součástí při upgradu aplikace na počítači, na němž je nainstalována aplikace Kaspersky Endpoint Agent. Automatický výběr součástí závisí na oprávněních uživatelského účtu, který aplikaci upgraduje.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru EXE nebo MSI pod systémovým účtem (SYSTEM), Kaspersky Endpoint Security získá přístup k aktuálním licencím řešení Kaspersky. Pokud je tedy v počítači nainstalována aplikace Kaspersky Endpoint Agent a aktivováno řešení EDR (KATA), instalační program aplikace Kaspersky Endpoint Security automaticky nakonfiguruje sadu součástí a vybere součást EDR (KATA). Tím se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent. Spuštění instalačního programu MSI pod systémovým účtem (SYSTEM) se obvykle provádí při upgradu prostřednictvím aktualizační služby Kaspersky nebo při nasazování instalačního balíčku prostřednictvím aplikace Kaspersky Security Center.

Pokud upgradujete aplikaci Kaspersky Endpoint Security pomocí souboru MSI pod uživatelským účtem bez oprávnění, Kaspersky Endpoint Security nemá přístup k aktuálním licencím řešení Kaspersky. V tomto případě aplikace Kaspersky Endpoint Security automaticky vybere součásti na základě sady součástí aplikace Kaspersky Endpoint Agent. Poté se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odstraní aplikaci Kaspersky Endpoint Agent.

Kaspersky Endpoint Security podporuje upgrade bez restartování počítače. Režim upgradu aplikace můžete vybrat ve vlastnostech zásad.

5 **Kontrola chodu aplikace**

Pokud je po instalaci nebo upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

- Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
- Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*. Pokud je stav součásti *Není součástí licence*, ujistěte se, že jste aktivovali funkci integrovaného agenta.
- V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.

6 **Kontrola připojení k serverů platformy Kaspersky Anti Targeted Attack Platform**

Zkontrolujte připojení k serverů platformy Kaspersky Anti Targeted Attack Platform. Postup:

1. Zkontrolujte, zda máte platný certifikát.
2. Zkontrolujte nastavení připojení k serveru.
3. Zkontrolujte protokol událostí.

   Pokud je navázáno spojení se serverem, aplikace odešle událost *Successful connection to the EDR Expert server*. Jestliže nedojde k žádné úspěšné události připojení a nenastanou žádné události s chybami připojení, zkontrolujte nastavení protokolu událostí a povolte odesílání událostí pro Endpoint Detection and Response (KATA).

Stav připojení k serveru neovlivňuje stav počítače v konzole aplikace Kaspersky Security Center. I když není k dispozici připojení k serveru, počítač může mít stav *OK*. Zkontrolujte protokol událostí a ověřte připojení k serveru.

7 **Kontrola výkonu**

Pokud se výkon počítače po instalaci nebo aktualizaci aplikace zpomalil, můžete optimalizovat přenos dat. Postup:

1. Zakažte součást EDR (KATA) a zkontrolujte, zda je snížení výkonu způsobeno EDR (KATA).
2. Pro důvěryhodné aplikace vypněte shromažďování telemetrie při vstupních operací konzoly (ve výchozím nastavení povoleno).
3. Přidejte aplikace, které snižují výkon počítače, na seznam důvěryhodných aplikací.
4. Kontaktujte technickou podporu společnosti Kaspersky. Odborníci podpory vám pomohou nakonfigurovat filtrování telemetrie v řešení Kaspersky Anti Targeted Attack Platform. Tím se sníží intenzita datového toku. Pokud je výkon vašeho počítače ovlivněn určitou aplikací, připojte k požadavku distribuční balíček této aplikace.

Endpoint Detection and Response Expert (on-premise)

Kaspersky Endpoint Security pro systém Windows podporuje integraci s řešením Managed Detection and Response Expert (on-premise). *Kaspersky Endpoint Detection and Response Expert (on-premise)* je podnikové řešení kybernetické bezpečnosti zahrnující aplikace společnosti Kaspersky, které umožňují organizaci bránit se před většinou typů kybernetických rizik a pokrývají nejdůležitější scénáře šíření hrozeb. Součásti EDR Expert (on-premise) jsou nasazeny na otevřené platformě OSMP (Open Single Management Platform). Tato platforma spouští scénáře pro různé platformy v jediném rozhraní a umožňuje integrovat aplikace Kaspersky s aplikacemi třetích stran do komplexního systému zabezpečení.

Jedním z ústředních prvků řešení je *SIEM*. SIEM sleduje události pocházející ze všech součástí a uvádí tyto události do vzájemného vztahu pomocí pravidel definovaných dodavatelem a uživatelem. EDR Expert (on-premise) se dívá na protokoly a telemetrii přijaté z podnikové infrastruktury za účelem automatického zjišťování útoků a umožňuje vyšetřovat incidenty pomocí jednotného grafu vyšetřování, který kombinuje všechny události shromážděné v aplikaci EDR Expert (on-premise), včetně událostí z aplikací společnosti Kaspersky a produkty pro zabezpečení informací třetích stran.

Pro reakci na pokročilé incidenty používá EDR Expert (on-premise) přednastavené a uživatelem definované scénáře. Můžete také použít akce odezvy z aplikací třetích stran a scénáře reakce, které zahrnují více aplikací.

Nástroje Threat Intelligence

Kaspersky Endpoint Detection and Response používá tyto nástroje po potlačování bezpečnostních hrozeb (Threat Intelligence):

- Integrace s portálem Kaspersky Threat Intelligence Portal, který obsahuje a zobrazuje informace o reputaci souborů a adres URL.
- Databáze Kaspersky Threats.

- Infrastruktura cloudových služeb Kaspersky Security Network (dále také jen „KSN"), která poskytuje přístup k informacím o souborech, webových stránkách a reputaci softwaru v reálném čase ze znalostní báze společnosti Kaspersky. Používání dat ze služby Kaspersky Security Network zaručuje rychlejší reakci aplikací společnosti Kaspersky na nové hrozby, zvyšuje účinnost některých součástí ochrany a snižuje pravděpodobnost falešně pozitivních výsledků.

Princip fungování řešení

Aplikace Kaspersky Endpoint Security se instaluje na jednotlivé počítače v podnikové IT infrastruktuře a nepřetržitě sleduje procesy, otevřená síťová připojení a upravované soubory. Informace o událostech v počítači (telemetrie) se odesílají na server EDR Expert (on-premise). V tomto případě aplikace Kaspersky Endpoint Security také odešle informace o hrozbách objevených aplikací a také informace o výsledcích zpracování těchto hrozeb na servery pro shromažďování telemetrie.

Integrace EDR Expert (on-premise) se konfiguruje v konzole aplikace Kaspersky Security Center. Integrovaný agent je pak spravován pomocí platformy OSMP (Open Single Management Platform), včetně spouštění úloh, správy objektů v karanténě, prohlížení zpráv a dalších akcí.

Konfigurace aplikace Kaspersky Endpoint Security pro fungování s řešením EDR Expert (on-premise)

Pro fungování s řešením EDR Expert (on-premise) lze použít následující konfigurace:

- **[KES+integrovaný agent]**. V této konfiguraci se Kaspersky Endpoint Security chová jako aplikace, která zajišťuje zabezpečení počítače, i jako aplikace pro fungování s řešením EDR Expert (on-premise). Integrovaný agent pro EDR Expert (on-premise) je k dispozici v aplikaci Kaspersky Endpoint Security pro systém Windows 12.11 nebo novější.
- **[EPP třetí strany+EDR Agent]**. V této konfiguraci je zabezpečení IT infrastruktury zajištěno platformou Endpoint Protection Platform (EPP) třetí strany. Interakci s řešením EDR Expert (on-premise) zajišťuje Kaspersky Endpoint Security v konfiguraci Endpoint Detection and Response Agent (EDR Agent). V této konfiguraci je EDR Agent kompatibilní s aplikacemi EPP třetích stran. EDR Agent pro řešení EDR Expert (on-premise) je k dispozici v aplikaci Kaspersky Endpoint Security pro systém Windows 12.11 nebo novější.

Integrace integrovaného agenta s řešením EDR Expert (on-premise)

Chcete-li integrovat s řešeními Kaspersky Endpoint Detection and Response Expert (on-premise), musíte přidat součást Endpoint Detection and Response Expert (on-premise) a nakonfigurovat aplikaci Kaspersky Endpoint Security.

Součásti EDR Optimum, EDR Expert a EDR Expert (on-premise) nejsou vzájemně kompatibilní.

Aby součást Endpoint Detection and Response Expert (on-premise) fungovala, musí být splněny tyto podmínky:

- Je nainstalována platforma OSMP (Open Single Management Platform).
- Je aktivována aplikace a na její funkčnost se vztahuje licence.
- Součást Endpoint Detection and Response Expert (on-premise) je zapnutá.
- Součásti aplikace, které zajišťují provoz řešení EDR Expert (on-premise), jsou povoleny a funkční. Provoz řešení EDR Expert (on-premise) zajišťují následující součásti:
  - Ochrana před souborovými hrozbami.
  - Ochrana před webovými hrozbami.
  - Ochrana před hrozbami v poště.
  - Prevence zneužití.
  - Detekce chování.
  - Prevence narušení hostitele.
  - Modul pro nápravu.
  - Adaptivní kontrola anomálií.

Nastavení Integrace EDR Expert (on-premise) zahrnuje následující kroky:

1. **Instalace součásti EDR Expert (on-premise)**

   Součást EDR Expert (on-premise) můžete vybrat během instalace nebo upgradu a dále použitím úlohy *Změna součástí aplikace*.

   Pro dokončení aktualizace aplikace novou součástí je nutné restartovat počítač.

2 **Aktivace součásti Kaspersky Endpoint Detection and Response Expert (on-premise)**

Musíte si koupit samostatnou licenci pro EDR Expert (on-premise) (doplněk součásti Kaspersky Endpoint Detection and Response Expert (on-premise)).

Funkce bude k dispozici poté, co pro Kaspersky Endpoint Detection and Response Expert (on-premise) zadáte samostatný klíč. V počítači tak jsou přidány dva klíče: klíč pro aplikaci Kaspersky Endpoint Security a klíč pro řešení Kaspersky Endpoint Detection and Response Expert (on-premise).

Fungování licence k samostatné funkci Endpoint Detection and Response Expert (on-premise) je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

Ověřte, zda je funkce EDR Expert (on-premise) součástí licence a je spuštěna v místním rozhraní aplikace.

3 **Připojování k serveru pro shromažďování telemetrie a odpovědní server**

Kaspersky Endpoint Detection and Response Expert (on-premise) vyžaduje důvěryhodné připojení mezi aplikací Kaspersky Endpoint Security a dvěma servery:

- *Server pro shromažďování telemetrie* je server, který je součástí řešení SIEM, které shromažďuje, normalizuje, uvádí do vzájemného vztahu, analyzuje a ukládá informace o událostech, k nimž dochází v počítači.
- *Odpovědní server* je server pro příjem a kontrolu dat, studium chování objektů a publikování výsledků těchto studií.

Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).

Ve výchozím nastavení Kaspersky Endpoint Security kontroluje pouze certifikát TLS serverů. Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače na serveru (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení serveru a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).

Jak připojit počítač Kaspersky Endpoint Security k součásti EDR Expert (on-premise) pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premise)**.
5. Zapněte přepínač **Endpoint Detection and Response Expert (on-premise) ENABLED**.
6. Chcete-li nakonfigurovat EDR Expert (on-premise), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 8.0 or later)**.
7. Nakonfigurujte připojení k *serverům pro shromažďování telemetrie*:

   a. V bloku **Connection to telemetry collection servers** klikněte na odkaz **Connection settings**.

   b. Nakonfigurujte připojení k serverům pro shromažďování telemetrie:

   - **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru.
   - **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).
   - **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

   c. Klikněte na tlačítko **OK**.

d. Přidejte servery pro shromažďování telemetrie. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

Můžete přidat více adres serveru pro shromažďování telemetrie. Kaspersky Endpoint Security se pokusí o připojení k serveru na první IP adrese. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit k druhé IP adrese v seznamu a tak dále.

e. V případě potřeby nakonfigurujte telemetrii.

8. Nakonfigurujte připojení k *odpovědním serverům*:

a. V bloku **Connection to response servers** nakonfigurujte nastavení **Send sync request to server every (min)**. Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace aplikace Kaspersky Endpoint Security přijímá úlohy reakce na hrozby a odesílá jejich výsledky.

b. Klikněte na odkaz **Connection settings**.

c. Nakonfigurujte připojení k odpovědním serverům:

- **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru.
- **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).
- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

  Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

d. Klikněte na tlačítko **OK**.

e. Přidejte odpovědní servery. Chcete-li to provést, zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

Můžete přidat více adres odpovědních serverů. Kaspersky Endpoint Security se pokusí o připojení k serveru na první IP adrese. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit k druhé IP adrese v seznamu a tak dále.

9. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Počítač je tak přidán do platformy OSMP (Open Single Management Platform). Provozní stav součásti zkontrolujete zobrazením *Report on status of application components*. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Endpoint Detection and Response Expert (on-premise)** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

Konfigurace nastavení telemetrie EDR Expert (on-premise)

Telemetrie je seznam událostí, ke kterým došlo na chráněném počítači. Kaspersky Endpoint Security analyzuje telemetrická data a během synchronizace je odesílá na servery pro shromažďování telemetrie. Telemetrické události přicházejí na server téměř nepřetržitě. Kaspersky Endpoint Security zahájí synchronizaci se serverem, když je splněna některá z následujících podmínek:

- Interval synchronizace vypršel.
- Počet událostí ve vyrovnávací paměti překročí horní limit.

Ve výchozím nastavení se tedy aplikace synchronizuje každých 30 sekund nebo vždy, když vyrovnávací paměť obsahuje 1024 událostí. Chování synchronizace můžete nakonfigurovat v zásadách aplikace Kaspersky Endpoint Security a vybrat optimální hodnoty, aby odpovídaly zatížení vaší sítě (viz pokyny níže).

Pokud mezi aplikací Kaspersky Endpoint Security a serverem není navázáno připojení, aplikace zařadí nové události do fronty. Po obnovení připojení odešle Kaspersky Endpoint Security události ve frontě na server ve správném pořadí. Aby nedošlo k přetížení serveru, může aplikace Kaspersky Endpoint Security některé události přeskočit. Chcete-li to povolit, můžete optimalizovat nastavení přenosu událostí, například nastavit maximální hodnotu událostí za hodinu (viz pokyny níže).

Chcete-li nakonfigurovat nastavení telemetrie, proveďte následující kroky:

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration → Endpoint Detection and Response Expert (on-premise)**.
5. Chcete-li nakonfigurovat EDR Expert (on-premise), ze seznamu řešení vyberte možnost **Endpoint Detection and Response Expert (version 8.0 or later)**.
6. Ujistěte se, že je v bloku **Data transmission settings** zaškrtnuto políčko **Send telemetry to telemetry collection servers**.
7. V případě potřeby zaškrtněte políčko **Send telemetry with IOA only**. *Indikátor útoku (IOA)* je pravidlo, které obsahuje popis podezřelého chování v systému, které může naznačovat cílený útok. Aplikace porovnává průběžné chování v systému s těmito pravidly a zaprotokoluje události, které ukazují na cílený útok. Aplikace používá technologii *kontrola streamování*, která umožňuje sledování těchto událostí v reálném čase.
8. V případě potřeby nakonfigurujte synchronizaci s nastavením serveru v bloku **Data transmission settings**:
   - **Maximum event transmission delay (sec)**. Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
   - **Maximum number of event packages**. Aplikace se synchronizuje se serverem, když se vyrovnávací paměť zaplní událostmi. Výchozí hodnota je 1024 událostí.
9. V případě potřeby zaškrtněte políčko **Enable request throttling** v bloku **Request throttling**.

   Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.
10. Konfigurace nastavení optimalizace pro odesílání událostí na server:
    - **Maximum number of events per hour**. Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
    - **Percentage of event limit excess**. Aplikace třídí události podle typu (například události „změny registru") a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.
11. V bloku **Connection to response servers** zadejte hodnotu pro parametr **Send sync request to server every (min)**.
12. Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.
13. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Výjimky z telemetrie EDR Expert (on-premise)

Chcete-li zlepšit výkon a optimalizovat přenos dat na server shromažďování telemetrie, můžete nakonfigurovat výjimky z telemetrie. Můžete se například rozhodnout neposílat data o síťové komunikaci u jednotlivých aplikací.

Použití příliš mnoha pravidel zahrnutí může zvýšit zátěž serveru pro shromažďování telemetrie a snížit výkon počítače. Doporučujeme přidávat pouze nezbytná pravidla.

Postup vytvoření výjimky z telemetrie ve webové konzole a cloudové konzole:

1. V hlavním okně webové konzoly vyberte kartu **Asset management → Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings → Telemetry Settings**.
5. Vyberte kartu **EDR Expert (on-premise) telemetry**.
6. V bloku **General exclusions** klikněte na tlačítko **Add**.

   Otevře se okno **Add exclusion rule**.
7. V případě potřeby změňte stav pravidla. Ve výchozím nastavení je pravidlo povoleno.
8. Zadejte název pravidla.

9. Vyberte akci, která se použije při aktivaci pravidla:

   - **Do not collect**. Filtrovaná událost bude z odesílané telemetrie vyloučena.
   - **Exclude IOA**. Událost aktivační události pravidla IoA bude z odesílané telemetrie vyloučena.

10. Pokud je vybrána možnost **Exclude IOA**, určete pravidla IoA, která mají být přidána do výjimek:

    - **Exclude all**. Po splnění zadané podmínky aplikace vyloučí z telemetrie události vygenerované na základě všech pravidel IoA.
    - **Exclude by GUID**. Zadejte identifikátor GUID pravidla IoA. Pomocí příkazu můžete určit více identifikátorů GUID `,`. Další informace o pravidlech IoA najdete v (místní) nápovědě pro EDR Expert.

11. Určete podmínku filtrování:

    a. Vyberte název pole, které chcete použít pro filtrování.

    b. Vyberte operátor (viz tabulka níže) a určete hodnotu, se kterou se bude hodnota pole z události porovnávat.

    Seznam podmíněných operátorů

Operátor	Popis
<	Pokud je hodnota pole menší než hodnota zadaná v podmínce, událost bude odfiltrována.
≤	Pokud je hodnota pole menší nebo rovna hodnotě zadané v podmínce, událost bude odfiltrována.
=	Pokud se hodnota pole rovná hodnotě zadané v podmínce, událost bude odfiltrována.
≥	Pokud je hodnota pole větší nebo rovna hodnotě zadané v podmínce, událost bude odfiltrována.
>	Pokud je hodnota pole větší než hodnota zadaná v podmínce, událost bude odfiltrována.
≠	Pokud hodnota pole není rovna hodnotě zadané v podmínce, událost bude odfiltrována.
is like	Pokud hodnota pole odpovídá masce zadané v podmínce, událost bude odfiltrována. Při zadávání masky podporuje aplikace znaky `*` a `?`:
is not like	Pokud hodnota pole neodpovídá masce zadané v podmínce, událost bude odfiltrována. Při zadávání masky podporuje aplikace znaky `*` a `?`:
one of	Pokud hodnota pole odpovídá jedné z hodnot v seznamu zadaném v podmínce, událost se považuje za filtrovanou.
none of	Pokud hodnota pole neodpovídá žádné z hodnot v seznamu zadaném v podmínce, událost se považuje za filtrovanou.
is like one of	Pokud hodnota pole odpovídá jedné z masek zadaných v podmínce, událost bude odfiltrována. Při zadávání masky podporuje aplikace znaky * a ?.
is not like one of	Pokud hodnota pole neodpovídá žádné z masek zadaných v podmínce, událost bude odfiltrována. Při zadávání masky podporuje aplikace znaky * a ?.
exists	Pokud je v události přítomno pole zadané v podmínce, událost bude odfiltrována.
not exists	Pokud pole zadané v podmínce není v události přítomno, událost bude odfiltrována.
contains	Pokud je v hodnotě pole přítomna hodnota zadaná v podmínce, událost bude odfiltrována.
is equal to	Pokud se hodnota pole rovná hodnotě zadané v podmínce, událost bude odfiltrována. Při kontrole se nerozlišují malá a velká písmena.
bitwise AND	Pokud je výsledek bitové operace AND (&) mezi hodnotou pole a hodnotou zadanou v podmínce 1, událost bude odfiltrována.

12. V případě potřeby můžete vytvořit složitá kritéria filtru přidáním více podmínek filtru a skupin podmínek. Do skupiny podmínek můžete také přidat vnořené podmínky a skupiny podmínek. Používat můžete následující operátory:

    - **AND** znamená, že filtr vybere události, které splňují všechny zadané podmínky.
    - **OR** znamená, že filtr vybere události, které splňují jednu ze zadaných podmínek.
    - **NOT** (chcete-li použít tento operátor, vyberte možnost **Add NOT before**) znamená, že filtr vybere události, které nesplňují žádnou ze zadaných podmínek.

    Podmínky a skupiny podmínek první úrovně se kombinují s operátorem **AND**.

13. Pokud máte v počítači spuštěnou platformu OSMP (Open Single Management Platform), můžete vytvořené pravidlo filtrování zkontrolovat. Chcete-li spustit kontrolu, klikněte na tlačítko **Check rule**.

    V okně, které se otevře, se zobrazí tabulka událostí filtrovaných podle vytvořeného pravidla. Další informace najdete v nápovědě k EDR Expert (cloud).

14. V případě potřeby v části **All event types** přidejte výjimky z telemetrie podle typu události.

    a. Klikněte na název typu události.

    b. V okně, které se otevře, klikněte na tlačítko **Set up manually**.

    c. V případě potřeby nakonfigurujte přenos telemetrie pro vybraný typ události pomocí přepínače **Send event**. Ve výchozím nastavení je přenos telemetrie povolen pro všechny typy událostí.

    d. V bloku **Exclusion rules** klikněte na tlačítko **Add**.

    Otevře se okno **Add exclusion rule**.

    e. Proveďte akce popsané v krocích 7–13 pro každé přidávané pravidlo.

15. U některých typů událostí můžete také přidat pravidla zahrnutí a rozšířit tak shromažďovanou telemetrii:

    a. V bloku **Inclusion rules** klikněte na tlačítko **Add**.

    Otevře se okno **Add inclusion rules**.

    b. Zadejte název pravidla.

    c. V části **Condition** zadejte hodnoty do zobrazených polí. Typ dostupných polí závisí na vybrané události.

    Pravidla výjimek mají přednost před pravidly zahrnutí.

16. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Export a import filtrů událostí EDR Expert (on-premise)

Seznam výjimek můžete exportovat do souboru JSON. Pak můžete soubor upravit, například přidat velké množství ID událostí. Funkci exportu/importu můžete také použít k zálohování filtrů událostí nebo k migraci seznamu na jiný server.

Použití příliš mnoha pravidel zahrnutí může zvýšit zátěž serveru pro shromažďování telemetrie a snížit výkon počítače. Doporučujeme přidávat pouze nezbytná pravidla.

Jak exportovat a importovat filtry událostí v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
5. V bloku **Nastavení telemetrie** → **Telemetrie EDR Expert (on-premise)** klikněte na tlačítko **Nastavení**.
6. Postup exportu filtrů událostí:

    a. Klikněte na tlačítko **Exportovat**.

    V okně, které se otevře, zadejte název souboru JSON, do kterého chcete exportovat filtry událostí, a vyberte složku, do které chcete tento soubor uložit.

    b. Uložte soubor.

    Aplikace Kaspersky Endpoint Security exportuje filtry událostí do souboru JSON.

7. Postup importu filtrů událostí:

    a. Klikněte na tlačítko **Importovat**.

    b. V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat filtry událostí.

    c. Otevřete soubor.

    Pokud už v počítači existují pravidla filtrování událostí, aplikace Kaspersky Endpoint Security je při importu nahradí.

8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak exportovat a importovat filtry událostí ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Telemetry Settings**.
5. Vyberte kartu **EDR Expert (on-premise) telemetry**.
6. Postup exportu filtrů událostí:
   a. Klikněte na tlačítko **Export**.
   b. V okně, které se otevře, zadejte název souboru JSON, do kterého chcete exportovat filtry událostí, a vyberte složku, do které chcete tento soubor uložit.
   c. Uložte soubor.
      Aplikace Kaspersky Endpoint Security exportuje filtry událostí do souboru JSON.
7. Postup importu filtrů událostí:
   a. Klikněte na tlačítko **Import**.
   b. V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat filtry událostí.
   c. Vyberte, jak chcete importovat pravidla filtrování událostí: přidáním do stávajících pravidel nebo odstraněním stávajících pravidel a nahrazením novými.
   d. Otevřete soubor.
8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Filtry událostí můžete také exportovat nebo importovat na příkazovém řádku.

Správa karantény

Karanténa je speciální místní úložiště v počítači. Uživatel může umístit do karantény soubory, které považuje za nebezpečné pro počítač. Soubory v karanténě jsou uloženy v šifrovaném stavu a neohrožují zabezpečení zařízení. Aplikace Kaspersky Endpoint Security použije karanténu, pouze je-li integrována s řešeními Kaspersky Detection and Response. V ostatních případech aplikace Kaspersky Endpoint Security umístí příslušný soubor do zálohy. Podrobnosti o správě karantény jako součásti řešení najdete v nápovědě k řešení Kaspersky Sandbox, nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum, nápovědě k řešení Kaspersky Endpoint Detection and Response Expert, nápovědě k řešení Kaspersky Anti Targeted Attack Platform a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise).

Kaspersky Endpoint Security používá ke karanténě souborů systémový účet (SYSTEM).

Nastavení karantény můžete konfigurovat pouze v konzole aplikace Kaspersky Security Center. Konzolu aplikace Kaspersky Security Center můžete také použít ke správě objektů v karanténě (obnovení, odstranění, přidání atd.). Místně, na počítači, můžete pouze obnovit objekt pomocí příkazového řádku.

Konfigurace maximální velikosti karantény

Ve výchozím nastavení je velikost karantény omezena na 1024 MB. Když karanténa dosáhne maximální velikosti, aplikace Kaspersky Endpoint Security zastaví odesílání souborů a vygeneruje událost *Nedostatek místa v úložišti karantény*. Abyste zabránili nedostatku místa na disku v karanténě, můžete nastavit prahovou hodnotu, při které Kaspersky Endpoint Security vygeneruje událost *V úložišti karantény není téměř volné místo*. Pro soubory v karanténě nelze dobu uchování nakonfigurovat tak, aby byly automaticky odebírány.

Je-li ve vaší organizaci nasazeno řešení Kaspersky Anti Targeted Attack Platform (EDR), doporučujeme zvětšit velikost karantény. Při provádění kontroly YARA může aplikace narazit na velký výpis paměti. Pokud velikost výpisu paměti přesáhne velikost karantény, kontrola YARA skončí s chybou a výpis paměti nebude umístěn do karantény. Doporučujeme nastavit velikost karantény rovnou celkové velikosti paměti RAM v počítači (například 8 GB) nebo zakázat limit velikosti karantény.

Jak nakonfigurovat maximální velikosti karantény v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Zprávy a úložiště**.

4. V bloku **Karanténa** nakonfigurujte velikost karantény:

   - **Omezit velikost karantény na N MB**. Pokud je toto políčko zaškrtnuto, maximální velikost karantény je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost nastavena na 1024 MB. Když karanténa dosáhne maximální velikosti, aplikace Kaspersky Endpoint Security odešle do aplikace Kaspersky Security Center událost *Nedostatek místa v úložišti karantény* a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace zastaví ukládání nových objektů do karantény. Karanténu musíte vyprazdňovat ručně.

     Není-li toto políčko zaškrtnuto, je velikost karantény omezena volným místem na disku.

   - **Upozornit, když úložiště karantény dosáhne N procent/a**. Prahová hodnota karantény. Můžete například nastavit prahovou hodnotu karantény na 50 %. Když karanténa dosáhne prahové hodnoty, aplikace Kaspersky Endpoint Security odešle odpovídající událost do aplikace Kaspersky Security Center a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace pokračuje v ukládání nových objektů do karantény.

     Není-li toto políčko zaškrtnuto, aplikace po dosažení limitu karantény negeneruje události.

5. Uložte změny.

Jak konfigurovat maximální velikosti karantény ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **General Settings** → **Reports and Storage**.

5. V bloku **Quarantine** nakonfigurujte velikost karantény:

   - **Limit the size of Quarantine**. Pokud je toto políčko zaškrtnuto, velikost karantény je omezena na zadanou hodnotu. Není-li toto políčko zaškrtnuto, je velikost karantény omezena volným místem na disku. To může být nutné u kontroly YARA, protože aplikace může uložit velký soubor výpisu paměti.

   - **Maximum size of Quarantine (MB)**. Pokud je toto políčko zaškrtnuto, maximální velikost karantény je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost nastavena na 1024 MB. Když karanténa dosáhne maximální velikosti, aplikace Kaspersky Endpoint Security odešle do aplikace Kaspersky Security Center událost *Nedostatek místa v úložišti karantény* a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace zastaví ukládání nových objektů do karantény. Karanténu musíte vyprazdňovat ručně.

     Není-li toto políčko zaškrtnuto, je velikost karantény omezena volným místem na disku.

   - **Notify when the Quarantine storage reaches (%)**. Prahová hodnota karantény. Můžete například nastavit prahovou hodnotu karantény na 50 %. Když karanténa dosáhne prahové hodnoty, aplikace Kaspersky Endpoint Security odešle odpovídající událost do aplikace Kaspersky Security Center a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace pokračuje v ukládání nových objektů do karantény.

6. Uložte změny.

Odesílání dat o souborech v karanténě do aplikace Kaspersky Security Center

Chcete-li provádět akce s objekty v karanténě ve webové konzole, musíte povolit odesílání dat souborů v karanténě na server pro správu. Můžete si například stáhnout soubor z karantény za účelem analýzy ve webové konzole. Aby fungovaly všechny funkce řešení Kaspersky Sandbox a Kaspersky Endpoint Detection and Response, musí být povoleno odesílání dat o souborech v karanténě.

Jak povolit přenos dat o souborech v karanténě do konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.

2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.

3. V okně zásad vyberte **Obecná nastavení** → **Zprávy a úložiště**.

4. V bloku **Přenos dat na server pro správu** klikněte na tlačítko **Nastavení**.

5. V okně, které se otevře, zaškrtněte políčko **Soubory v karanténě**.

6. Uložte změny.

Jak povolit přenos dat o souborech v karanténě ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **KSC Integration**.
5. V bloku **Data transfer to Administration Server** zaškrtněte políčko **About Quarantine files**.
6. Uložte změny.

Výsledkem je, že můžete v konzole aplikace Kaspersky Security Center zobrazit seznam souborů umístěných v karanténě. Webovou konzolu aplikace Kaspersky Security Center můžete použít ke správě objektů v karanténě (obnovení, odstranění, přidání atd.). Podrobnosti o práci s karanténou najdete v nápovědě k aplikaci Kaspersky Security Center.

Obnovení souborů z karantény

Ve výchozím nastavení aplikace Kaspersky Endpoint Security obnoví soubory do jejich původní složky. Pokud byla cílová složka odstraněna nebo uživatel nemá k této složce přístupová práva, aplikace umístí soubor do složky `%DataRoot%\QB\Restored`. Poté musíte soubor ručně přesunout do cílové složky.

Postup obnovení souborů z karantény:

1. V hlavním okně webové konzoly vyberte možnosti **Operations** → **Repositories** → **Quarantine**.
2. Tím otevřete seznam souborů v karanténě; v tomto seznamu vyberte soubory, které chcete obnovit, a klikněte na **Restore**.

Aplikace Kaspersky Endpoint Security tento soubor obnoví. Pokud cílová složka již obsahuje soubor se stejným názvem, aplikace obnovu souboru zruší. U řešení EDR Optimum a EDR Expert aplikace po obnovení soubor odstraní. U jiných řešení aplikace uchovávají kopii souboru v karanténě.

Monitorování akcí EDR

Kaspersky Endpoint Security pro systém Windows 12.9 zavádí centrum pro monitorování akcí EDR. *Centrum pro monitorování akcí EDR* je konzola, ve které můžete zobrazit historii součásti Reakce na hrozby pro všechna řešení Kaspersky Detection and Response. Pokud má vaše organizace nasazeno více řešení Detection and Response (například EDR Optimum a MDR), aplikace Kaspersky Endpoint Security zobrazí historii součásti Reakce na hrozby pro všechna řešení. To umožňuje analyzovat výkon řešení Detection and Response na samostatném počítači a optimalizovat nastavení těchto řešení.

Centrum pro monitorování poskytuje následující informace:

- Informace o úlohách součásti Reakce na hrozby (například úloze *Ukončit proces*)
- Změny pravidel Izolace sítě a Prevence spouštění

Pokud v reakci na hrozbu dojde k chybě související s přístupem k síťové sdílené položce, tato chyba je v zobrazené historii součásti Reakce na hrozby vynechána.

Přechod do centra pro monitorování akcí EDR:

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Assets (Devices)**.
2. Vyberte počítač, pro který chcete místní nastavení aplikace nakonfigurovat.
   Otevřou se vlastnosti počítače.
3. Vyberte kartu **Applications**.
4. Klikněte na tlačítko **Kaspersky Endpoint Security for Windows**.
   Otevřou se místní nastavení aplikace.
5. Vyberte kartu **Application settings**.
6. Přejděte na **Detection and Response** → **Response history**.

Otevře se konzola centra pro monitorování akcí EDR. Konzolu můžete použít k zobrazení stavů úlohy součásti Reakce na hrozby, trvání úlohy, změn pravidel a podrobností o iniciátorovi.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Aplikace Kaspersky Endpoint Security pro systém Windows podporuje řešení Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* je řešení pro správu bezpečnostních informací a událostí (SIEM) pro IT infrastrukturu organizací. KUMA umožňuje detekovat, analyzovat a zmírňovat bezpečnostní hrozby dříve, než mohou způsobit škodu.

Aplikace Kaspersky Endpoint Security se instaluje na jednotlivé počítače v podnikové IT infrastruktuře a nepřetržitě sleduje procesy, otevřená síťová připojení a upravované soubory. Informace o událostech v počítači (telemetrie) jsou odesílány na server KUMA (Kaspersky Unified Monitoring and Analysis Platform). KUMA ve své konzole zobrazuje události jako seznam bez označení, podobně jako protokol událostí systému Windows.

Kaspersky Endpoint Security neposkytuje u KUMA všechny funkce agenta. Aplikace pouze do KUMA odesílá události bez označení. Abyste získali přístup ke všem funkcím KUMA, musíte si zakoupit licenci a nasadit řešení v souladu s příručkou správce KUMA.

Integrace aplikace Kaspersky Endpoint Security s KUMA

Abyste mohli KUMA používat, musí být splněny následující podmínky:

- Kaspersky Security Center verze 14.2 nebo novější. Ve starších verzích aplikace Kaspersky Security Center není možné integraci KUMA aktivovat.
- Je aktivována aplikace a na její funkčnost se vztahuje licence.
- Je povolena součást pro integraci KUMA.

Nastavení Integrace KUMA zahrnuje následující kroky:

1. **Instalace součásti pro integraci KUMA**

   Součást pro integraci KUMA můžete vybrat během instalace nebo upgradu aplikace a dále použitím úlohy *Změna součástí aplikace*.

   Pro dokončení aktualizace aplikace novou součástí je nutné restartovat počítač.

2. **Aktivace KUMA**

   Kromě licence aplikace Kaspersky Endpoint Security (například Kaspersky Endpoint Security for Business Standard) potřebujete samostatnou licenci pro integraci aplikace Kaspersky Endpoint Security s KUMA (doplněk pro integraci KUMA s aplikací Kaspersky Endpoint Security pro systém Windows).

   Pokud instalujete aplikaci v režimu EDR Agent, potřebujete licenci pro integraci aplikace Kaspersky Endpoint Security s KUMA a licenci k řešení Kaspersky Anti Targeted Attack Platform (KATA) nebo licenci k řešení Kaspersky Managed Detection and Response (MDR). EDR Agent nelze nasadit pouze pro KUMA.

   Funkce se zpřístupní po přidání samostatného klíče KUMA. V počítači tak bude další aktivní klíč pro integraci aplikace Kaspersky Endpoint Security s KUMA.

   Fungování licence k samostatné funkci KUMA je stejné jako fungování licence k aplikaci Kaspersky Endpoint Security.

   Ověřte, zda je funkce KUMA součástí licence a je spuštěna v místním rozhraní aplikace.

3. **Připojování ke KUMA**

   Postup připojení počítače s aplikací Kaspersky Endpoint Security k řešení KUMA:

   1. V zásadách aplikace Kaspersky Endpoint Security přidejte adresy serveru KUMA a zadejte síťová nastavení připojení.
   2. V konzole KUMA přidejte kolektor s konektory typu tcp nebo udp a zadejte základní síťová nastavení připojení. Podrobnosti o správě kolektorů naleznete v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform.

   Můžete vytvořit důvěryhodné připojení mezi Kaspersky Endpoint Security a servery KUMA. Chcete-li nakonfigurovat důvěryhodné připojení, musíte použít certifikát TLS. Certifikát TLS můžete získat na serveru KUMA Core (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform). Poté musíte přidat certifikát TLS do aplikace Kaspersky Endpoint Security (viz pokyny níže).

Aby bylo připojení bezpečnější, můžete navíc povolit ověření počítače v KUMA (ověřování na obou stranách). Chcete-li povolit toto ověření, musíte zapnout ověřování na obou stranách v nastavení součásti KUMA a aplikace Kaspersky Endpoint Security. Chcete-li používat ověřování na obou stranách, budete také potřebovat kryptokontejner. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Certifikát s privátním klíčem ve formátu kontejneru PKCS#12 musíte vygenerovat u externí certifikační autority. Poté musíte přidat archiv PFX do konzoly KUMA a do aplikace Kaspersky Endpoint Security (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform).

Jak připojit počítač Kaspersky Endpoint Security k součásti KUMA pomocí konzoly pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte možnosti **Integrace KUMA**.
4. Zaškrtněte políčko **Integrace KUMA**.
5. V bloku **Nastavení integrace** zaškrtněte políčko **Povolit přenos událostí systému Windows na server KUMA**.
6. V případě potřeby zaškrtněte políčko **Použít šifrování TLS** v bloku **Nastavení pro připojení k serverům KUMA**.
7. Nakonfigurujte důvěryhodné připojení:
   a. Klikněte na tlačítko **Nastavení pro připojení k serverům KUMA**.
   b. Nakonfigurujte připojení k serveru:
      - **Doba vypršení časového limitu (s)**. Maximální časový limit odpovědi serveru KUMA. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru KUMA.
      - **Certifikát TLS serveru**. Certifikát TLS pro navázání důvěryhodného spojení se serverem KUMA. Certifikát TLS můžete získat v konzole Kaspersky Unified Monitoring and Analysis Platform (viz pokyny v řešení Kaspersky Unified Monitoring and Analysis Platform).
        Chcete-li vytvořit důvěryhodné připojení, v konzole KUMA v nastavení konektoru TCP musíte vybrat režim TLS **With verification** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform).
      - **Používat ověřování na obou stranách**. Ověřování na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a součástí KUMA. Chcete-li použít ověřování na obou stranách, musíte v konzole KUMA v nastavení konektoru tcp vybrat režim TLS **Custom PFX** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform). Poté musíte získat kryptokontejner a nastavit heslo pro ochranu kryptokontejneru. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Po konfiguraci nastavení součásti KUMA musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

        > Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

   c. Klikněte na tlačítko **OK**.
8. Přidejte servery KUMA:
   a. Klikněte na tlačítko **Přidat**.
      Otevře se formulář, do kterého můžete přidat server KUMA.
   b. Vyberte protokol pro připojení k serverům KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.
      Pokud vyberete protokol **HTTP/HTTPS**, ve výchozím nastavení aplikace používá pro připojení k serverům KUMA protokol HTTPS. Chcete-li používat protokol HTTP, musíte tento protokol ručně určit v adrese serveru (například `http://server.com`).
   c. Zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.
   d. Klikněte na tlačítko **OK**.

   Aplikace Kaspersky Endpoint Security se připojí k prvnímu serveru KUMA v seznamu. Pokud se připojení nezdaří, aplikace Kaspersky Endpoint Security se připojí k druhému serveru KUMA v seznamu a tak dále.
9. V případě potřeby nakonfigurujte nastavení **Maximální prodleva přenosu událostí (sek.)** v bloku **Nastavení přenosu dat**. Když zadaný čas vyprší, Kaspersky Endpoint Security se pokusí připojit ke stejnému serveru nebo se připojí k dalšímu serveru v seznamu, pokud existuje více serverů. Výchozí hodnota je 30 sekund.
10. Uložte změny.

[Jak připojit počítač Kaspersky Endpoint Security k součásti KUMA pomocí webové konzoly]

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Built-in Agents Configuration** → **KUMA Integration**.
5. Zapněte přepínač **KUMA Integration ENABLED**.
6. V případě potřeby zapněte přepínač **Use TLS encryption** v bloku **Server connection settings**.
7. Nakonfigurujte důvěryhodné připojení:

   a. Klikněte na tlačítko **Connection settings**.

   b. Nakonfigurujte připojení k serveru:

   - **Timeout (sec)**. Maximální časový limit odpovědi serveru KUMA. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru KUMA.
   - **Server TLS certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem KUMA. Certifikát TLS můžete získat v konzole Kaspersky Unified Monitoring and Analysis Platform (viz pokyny v řešení Kaspersky Unified Monitoring and Analysis Platform).

     Chcete-li vytvořit důvěryhodné připojení, v konzole KUMA v nastavení konektoru TCP musíte vybrat režim TLS **With verification** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform).
   - **Use two-way authentication**. Ověřování na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a součástí KUMA. Chcete-li použít ověřování na obou stranách, musíte v konzole KUMA v nastavení konektoru tcp vybrat režim TLS **Custom PFX** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform). Poté musíte získat kryptokontejner a nastavit heslo pro ochranu kryptokontejneru. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Po konfiguraci nastavení součásti KUMA musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

     > Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

   c. Klikněte na tlačítko **OK**.
8. Přidejte servery KUMA:

   a. Klikněte na tlačítko **Add**.

   Otevře se formulář, do kterého můžete přidat server KUMA.

   b. Vyberte protokol pro připojení k serverům KUMA: **HTTP / HTTPS**, **TCP**, **UDP**.

   Pokud vyberete protokol **HTTP/HTTPS**, ve výchozím nastavení aplikace používá pro připojení k serverům KUMA protokol HTTPS. Chcete-li používat protokol HTTP, musíte tento protocol ručně určit v adrese serveru (například `http://server.com`).

   c. Zadejte adresu serveru (IPv4, IPv6) a port pro připojení k serveru.

   d. Klikněte na tlačítko **OK**.

   Aplikace Kaspersky Endpoint Security se připojí k prvnímu serveru KUMA v seznamu. Pokud se připojení nezdaří, aplikace Kaspersky Endpoint Security se připojí k druhému serveru KUMA v seznamu a tak dále.
9. V případě potřeby nakonfigurujte nastavení **Maximum delay when sending events (sec)** v bloku **Server connection settings**. Když zadaný čas vyprší, Kaspersky Endpoint Security se pokusí připojit ke stejnému serveru nebo se připojí k dalšímu serveru v seznamu, pokud existuje více serverů. Výchozí hodnota je 30 sekund.
10. Uložte změny.

Správnou konfiguraci integrace KUMA můžete ověřit v konzole KUMA (podrobnosti najdete v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform). Informace o provozním stavu součásti vám poskytne *Report on status of application components* v konzole aplikace Kaspersky Security Center. Provozní stav součásti můžete také zobrazit ve zprávách v místním rozhraní aplikace Kaspersky Endpoint Security. Součást **Integrace KUMA** bude přidána do seznamu součástí aplikace Kaspersky Endpoint Security.

4 **Povolení odesílání telemetrie na server KUMA**

Ve výchozím nastavení je odesílání událostí na server KUMA zakázáno. Aby server KUMA fungoval správně, musíte povolit odesílání telemetrie. Zdroj událostí můžete vybrat ze standardních protokolů: *Application*, *Security* nebo *System*.

Jak povolit odesílání telemetrie na server KUMA v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
5. V bloku **Nastavení telemetrie** → **Telemetrie KUMA** klikněte na tlačítko **Nastavení**.
6. Vyberte protokoly událostí, které chcete použít jako zdroje událostí: *Application*, *Security* nebo *System*.
   Kromě standardních protokolů můžete určit a protokol aplikace třetí strany.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak povolit odesílání telemetrie na server KUMA ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Telemetry Settings**.
5. Vyberte kartu **KUMA telemetry**.
6. Vyberte protokoly událostí, které chcete použít jako zdroje událostí: *Application*, *Security* nebo *System*.
   Kromě standardních protokolů můžete určit a protokol aplikace třetí strany.
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Filtrování událostí, které mají být odeslány do sítě KUMA

Ve výchozím nastavení je odesílání událostí na server KUMA zakázáno. Aby server KUMA fungoval správně, musíte povolit odesílání telemetrie. Zdroj událostí můžete vybrat ze standardních protokolů: *Application*, *Security* nebo *System*. Chcete-li zvýšit výkon a optimalizovat přenos dat na server KUMA, můžete ručně přidat jednotlivé události nebo z ní vyloučit jednotlivé události. Můžete například vyloučit události sysmon.

Jak vytvořit seznam událostí, které mají být odeslány do sítě KUMA, v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
5. V bloku **Nastavení telemetrie** → **Telemetrie KUMA** klikněte na tlačítko **Nastavení**.
6. V okně, které se zobrazí, nakonfigurujte filtry událostí, které mají být odesílány do sítě KUMA.
   Můžete nakonfigurovat filtrování událostí pro standardní protokoly *Application*, *Security*, *System* nebo ručně přidat další protokol.
   a. Klikněte na tlačítko **Přidat** nebo otevřete vlastnosti protokolu.
   b. Vyberte režim odeslání událostí:
   - **Odesílat všechny události**. V tomto režimu aplikace odesílá všechny události z protokolu systému Windows kromě událostí přidaných do pravidel výjimek.

- **Odesílat pouze vybrané události**. V tomto režimu aplikace odesílá pouze události přidané do pravidel zahrnutí.

c. Vytvořte seznamy pravidel výjimek nebo pravidel zahrnutí pro příslušný režim odesílání událostí.

Chcete-li přidat pravidla, musíte zadat ID události v protokolu událostí systému Windows. V pravidle můžete uvést více ID událostí. Pokud chcete zadat více ID událostí, použijte znak čárky (,).

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak vytvořit seznam událostí, které mají být odeslány do sítě KUMA, ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Telemetry Settings**.
5. Vyberte kartu **KUMA telemetry**.
6. V okně, které se zobrazí, nakonfigurujte filtry událostí, které mají být odesílány do sítě KUMA.
   Můžete nakonfigurovat filtrování událostí pro standardní protokoly *Application*, *Security*, *System* nebo ručně přidat další protokol.
   a. Klikněte na tlačítko **Add** nebo otevřete vlastnosti protokolu.
   b. Vyberte režim odeslání událostí:
      - **Send all events**. V tomto režimu aplikace odesílá všechny události z protokolu systému Windows kromě událostí přidaných do pravidel výjimek.
      - **Send only selected events**. V tomto režimu aplikace odesílá pouze události přidané do pravidel zahrnutí.
   c. Vytvořte seznamy pravidel výjimek nebo pravidel zahrnutí pro příslušný režim odesílání událostí.
      Chcete-li přidat pravidla, musíte zadat ID události v protokolu událostí systému Windows. V pravidle můžete uvést více ID událostí. Pokud chcete zadat více ID událostí, použijte znak čárky (,).
7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Export a import filtrů událostí KUMA

Seznam výjimek můžete exportovat do souboru JSON. Pak můžete soubor upravit, například přidat velké množství ID událostí. Funkci exportu/importu můžete také použít k zálohování filtrů událostí nebo k migraci seznamu na jiný server.

Použití příliš mnoha pravidel může zvýšit zátěž serveru KUMA a snížit výkon počítače. Doporučujeme přidávat pouze nezbytná pravidla.

Jak exportovat a importovat filtry událostí v konzole pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzoly vyberte možnost **Policies**.
3. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
4. V okně zásad vyberte **Obecná nastavení** → **Výjimky a typy objektů**.
5. V bloku **Nastavení telemetrie** → **Telemetrie KUMA** klikněte na tlačítko **Nastavení**.
6. Postup exportu filtrů událostí:
   a. Vyberte protokoly událostí s filtry, které chcete exportovat.
   b. Klikněte na tlačítko → **Exportovat**.

c. V okně, které se otevře, zadejte název souboru JSON, do kterého chcete exportovat filtry událostí, a vyberte složku, do které chcete tento soubor uložit.

d. Uložte soubor.

Aplikace Kaspersky Endpoint Security exportuje filtry událostí do souboru JSON.

7. Postup importu filtrů událostí:

a. Klikněte na tlačítko → **Importovat**.

b. V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat filtry událostí.

c. Otevřete soubor.

Pokud už v počítači existují pravidla filtrování událostí, aplikace Kaspersky Endpoint Security je při importu nahradí.

8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Jak exportovat a importovat filtry událostí ve webové konzole

1. V hlavním okně webové konzoly vyberte kartu **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Telemetry Settings**.
5. Vyberte kartu **KUMA telemetry**.
6. Postup exportu filtrů událostí:

a. Vyberte protokoly událostí s filtry, které chcete exportovat.

b. Klikněte na tlačítko → **Export**.

c. V okně, které se otevře, zadejte název souboru JSON, do kterého chcete exportovat filtry událostí, a vyberte složku, do které chcete tento soubor uložit.

d. Uložte soubor.

Aplikace Kaspersky Endpoint Security exportuje filtry událostí do souboru JSON.

7. Postup importu filtrů událostí:

a. Klikněte na tlačítko → **Import**.

b. V okně, které se otevře, vyberte soubor JSON, ze kterého chcete importovat filtry událostí.

c. Otevřete soubor.

Pokud už v počítači existují pravidla filtrování událostí, aplikace Kaspersky Endpoint Security je při importu nahradí.

8. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.

Filtry událostí můžete také exportovat nebo importovat na příkazovém řádku.

Průvodce migrací z KSWS na KES

Od verze 11.8.0 aplikace Kaspersky Endpoint Security podporuje základní funkce řešení Kaspersky Security for Windows Server (KSWS). *Kaspersky Security for Windows Server* chrání servery s operačními systémy Microsoft Windows a síťová úložiště proti virům a dalším hrozbám zabezpečení počítače, kterým jsou servery a síťová úložiště vystaveny při výměně souborů. Podrobné informace o tom, jak řešení funguje, najdete v nápovědě k aplikaci Kaspersky Security for Windows Server. Od aplikace Kaspersky Endpoint Security 11.8.0 můžete migrovat z aplikace Kaspersky Security for Windows Server na aplikaci Kaspersky Endpoint Security pro systém Windows a používat stejné řešení k ochraně pracovních stanic i serverů.

Požadavky na software

Před zahájením migrace z KSWS na KES se ujistěte, že váš server splňuje požadavky aplikace Kaspersky Endpoint Security pro systém Windows na hardware a software. Seznamy podporovaných verzí operačního systému se pro KES a KSWS liší. KES například nepodporuje servery se systémem Windows Server 2003.

Minimální požadavky na software pro migraci z KSWS na KES:

- Kaspersky Endpoint Security pro systém Windows 12.0
- Kaspersky Security 11.0.1 for Windows Server

  Pokud máte nainstalovanou starší verzi aplikace Kaspersky Security for Windows Server, doporučujeme upgradovat aplikaci na nejnovější verzi. Průvodce převodem zásad a úloh nepodporuje starší verze aplikace Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  Pokud máte nainstalovanou starší verzi aplikace Kaspersky Security Center, aktualizujte ji na verzi 14.2 nebo novější. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh umožňuje migrovat zásady do profilu, nikoli do zásady. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh také umožňuje migrovat širší rozsah nastavení zásad.
- Kaspersky Endpoint Agent 3.10

  Pokud máte nainstalovanou starší verzi aplikace Kaspersky Endpoint Agent, doporučujeme upgradovat aplikaci na nejnovější verzi. Kaspersky Endpoint Security podporuje migraci konfigurace [KSWS+KEA] na [KES+integrovaného] počínaje aplikací Kaspersky Endpoint Agent 3.10.

Doporučení k migraci

Při migraci z KSWS na KES dodržujte následující doporučení:

- Naplánujte si čas migrace KSWS na KES předem. Vyberte si čas, kdy servery pracují s nejmenší zátěží, například o víkendu.
- Po migraci postupně zapínejte součásti aplikace. Tzn. například začněte povolením samotné součásti Ochrana před souborovými hrozbami, poté povolte další součásti ochrany, poté povolte součásti kontroly atd. V každém kroku se musíte ujistit, že aplikace funguje správně, a sledovat výkon serveru. Architektura KES se liší od KSWS, proto se může odlišně chovat i operační systém.
- Migraci provádějte postupně. Nejprve proveďte migraci jednoho serveru, poté více serverů a poté proveďte migraci na všech serverech organizace.
- Migrujte různé typy serverů samostatně. To znamená například nejprve migrujte databázové servery, poté poštovní servery atd.
- Migrace na vysoce zatížených serverech je nutno brát v úvahu některé zvláštní aspekty.

Kroky migrace

Migrace z KSWS na KES se provádí poloautomaticky. To je nutné z důvodu rozdílných architektur aplikací. Chcete-li migrovat nastavení zásad, musíte spustit průvodce hromadným převodem zásad a úloh (průvodce migrací). Po migraci nastavení zásad musíte ručně nakonfigurovat nastavení, která průvodce migrací nemůže migrovat automaticky (například nastavení ochrany heslem). Po migraci je také doporučeno zkontrolovat, zda průvodce migrací správně migroval všechna nastavení.

Proveďte migraci z KSWS na KES v následujícím pořadí:

1. **Migrace úloh a zásad KSWS**

   Po migraci zásad a úloh musíte provést další konfigurační kroky. Doporučujeme také ujistit se, že Kaspersky Endpoint Security poskytuje potřebnou úroveň zabezpečení po migraci z KSWS.

   Průvodce hromadným převodem zásad a úloh pro aplikaci Kaspersky Security for Windows Server je k dispozici pouze v konzole pro správu (MMC). Nastavení zásad a úloh nelze migrovat ve webové konzole a v cloudové konzole aplikace Kaspersky Security Center.

2. **Nainstalujte aplikaci Kaspersky Endpoint Security**

   Aplikaci Kaspersky Endpoint Security můžete nainstalovat následujícími způsoby:

   - Instalace KES po odebrání KSWS (doporučeno).

     Nástroj kavremover nepodporuje správu KSWS.

   - Instalace KES na KSWS.
3. **Aktivujte KES pomocí klíče KSWS**

4 **Ověření, zda je aplikace po migraci funkční**

Po migraci z KSWS na KES se ujistěte, že aplikace funguje správně. V konzole kontrolujte stav serveru (měl by být *OK*). Ujistěte se, že pro aplikaci nejsou hlášeny žádné chyby, zkontrolujte také čas posledního připojení k serveru pro správu, čas poslední aktualizace databáze a stav ochrany serveru.

Zvláštní pozornost věnujte migraci seznamů výjimek, důvěryhodných aplikací, důvěryhodných webových adres a pravidel součásti Kontrola aplikací.

Shoda součástí KSWS a KES

Při migraci z KSWS na KES se sada součástí migruje pouze tehdy, když se aplikace instaluje lokálně.

Shoda součástí Kaspersky Security for Windows Server a Kaspersky Endpoint Security pro systém Windows

Součást aplikace Kaspersky Security for Windows Server	Součást aplikace Kaspersky Endpoint Security pro systém Windows
Basic functionality	Jádro aplikace
Log Inspection	Kontrola protokolu
Device Control	Kontrola zařízení
Firewall Management	*(není podporováno)* Funkce brány firewall KSWS provádí systémová brána firewall. V KES je za funkčnost brány firewall zodpovědná samostatná součást. Po migraci můžete nakonfigurovat bránu firewall aplikace Kaspersky Endpoint Security.
File Integrity Monitor	Monitorování integrity systému
Exploit Prevention	Prevence zneužití
System Tray Icon	*(není podporováno)* Uživatelskou interakci můžete nakonfigurovat v nastavení rozhraní aplikace.
Integration with Kaspersky Security Center	Network Agent Connector
Endpoint Agent	*(není podporováno)* V aplikaci Kaspersky Endpoint Security 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady Kaspersky Endpoint Security. Distribuční balíček Kaspersky Endpoint Agent si musíte stáhnout samostatně.
Network Threat Protection	Ochrana před síťovými hrozbami
Anti-Cryptor	Detekce chování
Anti-Cryptor for NetApp	*(není podporováno)*
Traffic Security	Ochrana před webovými hrozbami Ochrana před hrozbami v poště Kontrola webu
On-Demand Scan	Jádro aplikace
ICAP Network Storage Protection	*(není podporováno)* Kaspersky Endpoint Security nepodporuje součásti Ochrana síťově připojených úložišť. Pokud tyto součásti potřebujete, můžete pokračovat v používání aplikace Kaspersky Security for Windows Server.
RPC Network Storage Protection	*(není podporováno)* Kaspersky Endpoint Security nepodporuje součásti Ochrana síťově připojených úložišť. Pokud tyto součásti potřebujete, můžete pokračovat v používání aplikace Kaspersky Security for Windows Server.
Real-Time File Protection	Ochrana před souborovými hrozbami
Script Monitoring	*(není podporováno)* Sledování skriptů je řešeno jinými součástmi, např. Ochrana AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	Kontrola aplikací
Performance counters	*(není podporováno)*

Shoda nastavení KSWS a KES

Rozbalit vše | Sbalit vše

Při migraci zásad a úloh je aplikace KES nakonfigurována v souladu s nastavením KSWS. Nastavení součástí aplikace, které KSWS nemá, jsou nastavena na výchozí hodnoty.

Application settings

Scalability, interface and scanning settings

Nastavení aplikace nejsou v aplikaci Kaspersky Endpoint Security pro systém Windows podporována.

Nastavení aplikace

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Scalability settings	*(nemigruje)* Kaspersky Endpoint Security spravuje všechny pracovní procesy.
Show System Tray Icon	*(nemigruje)* V klientském počítači je standardně 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. Uživatelskou interakci můžete nakonfigurovat v nastavení rozhraní aplikace.
Restore file attributes after scanning	*(nemigruje)* Aplikace Kaspersky Endpoint Security po kontrole souboru automaticky obnoví atributy souboru.
Limit CPU usage for scanning threads	*(nemigruje)* Kaspersky Endpoint Security neomezuje využití procesoru při kontrole. Úlohu můžete nakonfigurovat, aby se spouštěla, když počítač pracuje s minimální zátěží.
Folder for temporary files created during scanning	*(nemigruje)* Kaspersky Endpoint Security umístí dočasné soubory do složky `C:\Windows\Temp`.
HSM system settings	*(nemigruje)* Aplikace Kaspersky Endpoint Security nepodporuje systémy HSM.

Security and reliability

Nastavení zabezpečení KSWS jsou migrována do části **Obecná nastavení**, pododdílů Nastavení aplikace a Rozhraní.

Nastavení zabezpečení aplikace

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Protect application processes from external threats	**Povolit sebeobranu** (pododdíl **Nastavení aplikace**)
Apply password protection	*(nemigruje)* Kaspersky Endpoint Security má integrovanou funkci Ochrana heslem (pododdíl **Rozhraní**).
Perform task recovery	*(nemigruje)* Kaspersky Endpoint Security pouze automaticky obnoví úlohy *Kontrola malwaru*. Aplikace Kaspersky Endpoint Security spustí další úlohy podle plánu.
Do not start scheduled scan tasks	**Odložit naplánované úlohy při napájení z baterie** (pododdíl **Nastavení aplikace**)
Stop current scan tasks	*(nemigruje)* Když je počítač napájen UPS, aplikace Kaspersky Endpoint Security nezastaví úlohy kontroly, které jsou již spuštěné.

Connection settings

Nastavení interakce se serverem pro správu jsou migrována do části **Obecná nastavení**, pododdílů Nastavení sítě a Nastavení aplikace.

Nastavení interakce se serverem pro správu

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Proxy server settings	**Nastavení proxy serveru** (pododdíl **Nastavení sítě**)

Do not use proxy server for local addresses	**Obcházet proxy server u místních adres** (pododdíl **Nastavení sítě**)
Proxy server authentication settings	**Použít ověření proxy serveru** (pododdíl **Nastavení sítě**) Heslo pro ověření proxy serveru není migrováno. Po migraci zásady je nutno heslo zadat ručně.
Use Kaspersky Security Center as a proxy server when activating the application	**Použít Kaspersky Security Center jako proxy server pro aktivaci** (pododdíl **Nastavení aplikace**)

Run local system tasks

Kaspersky Endpoint Security ignoruje nastavení pro spouštění místních systémových úloh aplikace Kaspersky Security for Windows Server. Používání místních úloh KES můžete nakonfigurovat v části **Místní úlohy**, **Správa úloh**. Můžete také nakonfigurovat plán pro spouštění úloh *Kontrola malwaru* a *Aktualizace databází a modulů aplikace* ve vlastnostech těchto úloh.

Supplementary

Trusted zone

Nastavení důvěryhodné zóny KSWS jsou migrována do části **Obecná nastavení**, pododdílu **Výjimky**.

Nastavení důvěryhodné zóny

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Object to scan (Exclusions)	**Výjimky z kontroly** (Výjimky z kontroly) Metody používané aplikacemi KSWS a KES pro výběr objektů se liší. Při migraci KES podporuje výjimky definované jako jednotlivé soubory nebo cesty k souboru/složce. Pokud má KSWS výjimky nakonfigurované jako předdefinovaná oblast nebo adresa URL skriptu, tyto výjimky se nemigrují. Po migraci musíte tyto výjimky přidat ručně. Výjimky a předdefinované oblasti je nutno nakonfigurovat v nastavení úlohy *Kontrola malwaru*. Výjimky jako webové adresy skriptů musíte přidat k důvěryhodným webovým adresám součásti Ochrana před webovými hrozbami.
Apply also to subfolders (Exclusions)	**Včetně podsložek** (Výjimky z kontroly)
Objects to detect (Exclusions)	**Typ zjištěného objektu** (Výjimky z kontroly)
Exclusion usage scope (Exclusions)	**Součásti ochrany** (Výjimky z kontroly) Pokud je v KSWS vybrána alespoň jedna součást, KES použije výjimky na všechny součásti aplikace.
Comment (Exclusions)	**Poznámka** (Výjimky z kontroly)
Trusted process (Trusted process)	**Důvěryhodné aplikace** Metody výběru důvěryhodných procesů/aplikací se u KSWS a KES liší. Při migraci KES podporuje důvěryhodné aplikace nakonfigurované jako cesta ke spustitelnému souboru nebo maska. Pokud má KSWS důvěryhodné procesy nakonfigurované jako hodnota hash souboru, tyto důvěryhodné procesy nebudou migrovány. Po migraci musíte tyto důvěryhodné procesy přidat ručně.
Do not check file backup operations (Trusted process)	**Nemonitorovat činnost aplikace** (Důvěryhodné aplikace)

Removable drives scan

Nastavení kontroly vyměnitelných jednotek jsou migrována do části **Místní úlohy**, pododdílu **Kontrola vyměnitelných jednotek**.

Nastavení kontroly vyměnitelných jednotek

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Scan removable drives on connection via USB	**Akce při připojení vyměnitelné jednotky**
Scan removable drives if its stored data volume does not exceed (MB)	**Maximální velikost vyměnitelné jednotky**
Scan with security level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Akce při připojení vyměnitelné jednotky**: • **Maximální ochrana** • **Doporučená**. Úrovně zabezpečení KSWS odpovídají režimům kontroly KES takto: • Maximum protection – Maximální ochrana. • Recommended – Doporučená. • Maximum performance – Doporučená.

User permissions for application management

Kaspersky Endpoint Security nepodporuje přidělování uživatelských přístupových oprávnění pro správu aplikací a správu aplikačních služeb. Můžete nakonfigurovat nastavení přístupu pro uživatele a skupiny uživatelů pro správu aplikace v aplikaci Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

Kaspersky Endpoint Security nepodporuje přidělování uživatelských přístupových oprávnění pro správu aplikací a správu aplikačních služeb. Můžete nakonfigurovat nastavení přístupu pro uživatele a skupiny uživatelů pro správu aplikace v aplikaci Kaspersky Security Center.

Storages

Nastavení úložiště KSWS jsou migrována do části **Obecná nastavení**, pododdílu **Zprávy a úložiště**, a do části **Základní ochrana před hrozbami**, pododdílu **Ochrana před síťovými hrozbami**.

Nastavení úložiště

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Backup folder	*(nemigruje)* Kaspersky Endpoint Security ukládá záložní kopie souborů do složky `C:\ProgramData\Kaspersky Lab\KES.14.0\QB`.
Maximum Backup size (MB)	**Omezit velikost zálohy na N MB** (část **Obecná nastavení** → **Zprávy a úložiště**)
Threshold value for space available (MB)	*(nemigruje)* Kaspersky Endpoint Security zaznamenává do protokolu událost *V úložišti karantény není téměř volné místo* při dosažení prahové hodnoty 50 %.
Target folder for restoring objects	*(nemigruje)* Kaspersky Endpoint Security obnoví soubory do jejich původní složky.
Quarantine folder	*(nemigruje)* Kaspersky Endpoint Security ukládá záložní kopie souborů do složky `C:\ProgramData\Kaspersky Lab\KES.14.0\QB`.
Maximum Quarantine size (MB)	*(nemigruje)* Kaspersky Endpoint Security používá zálohu k ukládání pravděpodobně infikovaných objektů. Během migrace aplikace Kaspersky Endpoint Security ignoruje nastavení karantény.
Threshold value for space available (MB)	*(nemigruje)* Kaspersky Endpoint Security používá zálohu k ukládání pravděpodobně infikovaných objektů. Během migrace aplikace Kaspersky Endpoint Security ignoruje nastavení karantény.
Target folder for restoring objects	*(nemigruje)* Kaspersky Endpoint Security obnoví soubory do jejich původní složky.

Unblock automatically in N	**Blokovat útočící zařízení po dobu N min** (část **Základní ochrana před hrozbami → Ochrana před síťovými hrozbami**)

Real-time server protection

Real-Time File Protection

Nastavení ochrany souborů v reálném čase KSWS jsou migrována do části **Základní ochrana před hrozbami**, pododdílu Ochrana před souborovými hrozbami.

Nastavení ochrany souborů v reálném čase

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Objects protection mode: • **Smart mode** • **When run** • **On access** • **On access and modification**	**Režim kontroly**: • **Chytrý režim** • **Při provedení** • **Při přístupu** • **Při přístupu a změnách**.
Deeper analysis of launching processes	*(nemigruje)* Kaspersky Endpoint Security podporuje pouze jeden režim analýzy, režim Optimal.
Heuristic analyzer: • **Light** • **Medium** • **Deep**	**Heuristická analýza**: • **lehká kontrola** • **střední kontrola** • **hloubková kontrola**.
Apply Trusted Zone	*(nemigruje)* Kaspersky Endpoint Security použije důvěryhodnou zónu na všechny součásti. Výjimky můžete nakonfigurovat v nastavení důvěryhodné zóny.
Use KSN for protection	*(nemigruje)* Kaspersky Endpoint Security používá KSN pro všechny součásti aplikace.
Block access to network shared resources for the hosts that show malicious activity	*(nemigruje)* Ve výchozím nastavení Kaspersky Endpoint Security blokuje přístup ke sdíleným síťovým zdrojům pro hostitele, kteří vykazují škodlivou aktivitu.
Launch critical areas scan when active infection is detected	*(nemigruje)* Kaspersky Endpoint Security nespustí úlohu kontroly kritických oblastí, když je zjištěna aktivní infekce.
Use Kaspersky Sandbox for protection	*(nemigruje)* Ve výchozím nastavení Kaspersky Endpoint Security odesílá objekty ke kontrole do řešení Kaspersky Sandbox.
Protection scope	**Rozsah ochrany**
Schedule settings	*(nemigruje)* Kaspersky Endpoint Security používá svůj vlastní plán pro pozastavení součásti Ochrana před souborovými hrozbami.

KSN Usage

Nastavení KSWS pro aplikaci Kaspersky Security Network jsou migrována do části **Rozšířená ochrana před hrozbami**, pododdílu Kaspersky Security Network.

Nastavení služby Kaspersky Security Network

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**Prohlášení o Kaspersky Security Network**

	Kaspersky Endpoint Security vyžaduje souhlas s prohlášením o Kaspersky Security Network, když je instalována aplikace, jsou vytvořeny nové zásady nebo je povoleno používání služby Kaspersky Security Network.
Send data about scanned files	*(nemigruje)* Pokud je povolena služba KSN, aplikace Kaspersky Endpoint Security automaticky odesílá data o kontrolovaných souborech.
Send data about requested URLs	*(nemigruje)* Pokud je povolena služba KSN, aplikace Kaspersky Endpoint Security automaticky odesílá data vyžádaných adresách URL.
Send Kaspersky Security Network statistics	**Povolit rozšířený režim KSN**
Accept the terms of the Kaspersky Managed Protection Statement	*(nemigruje)* Kaspersky Endpoint Security nezahrnuje službu KMP.
Action to perform on KSN untrusted objects	*(nemigruje)* Akci při detekci hrozeb můžete nakonfigurovat v nastavení součásti ochrany a nastavení úlohy kontroly.
Do not calculate checksum before sending to KSN if file size exceeds N MB	*(nemigruje)* Omezení kontroly velkých souborů můžete nakonfigurovat v nastavení součásti ochrany a nastavení úlohy kontroly.
Use Kaspersky Security Center as KSN Proxy	**Použít jako proxy server KSN server pro správu**
Schedule settings	*(nemigruje)* Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Traffic Security

Nastavení zabezpečení provozu KSWS jsou migrována do části **Základní ochrana před hrozbami**, Ochrana před webovými hrozbami a pododdílu Ochrana před hrozbami v poště, části **Kontrolní prvky zabezpečení**, pododdílu Kontrola webu, části **Obecná nastavení**, pododdílu Nastavení sítě.

Zabezpečení přenosů

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Apply URL-based rules	**Kontrola webu** (pododdíl **Kontrola webu**) Pravidla založená na adresách URL jsou v aplikaci Kaspersky Endpoint Security migrována do samostatných pravidel.
Apply certificate-based rules	*(nemigruje)* Aplikace Kaspersky Endpoint Security nepodporuje pravidla založená na certifikátech.
Apply rules for web traffic category control	**Kontrola webu** (pododdíl **Kontrola webu**) Pravidla blokování pro řízení kategorií webového provozu jsou v aplikaci Kaspersky Endpoint Security migrována do jediného pravidla blokování. Kaspersky Endpoint Security ignoruje povolená pravidla pro řízení kategorií. Shoda kategorií KSWS a KES je uvedena níže.
Allow access if the web page can not be categorized	*(nemigruje)* Kaspersky Endpoint Security povolí přístup, pokud webovou stránku nelze kategorizovat.
Allow access to legitimate web resources that can be used to damage a protected device	*(nemigruje)* Kaspersky Endpoint Security povolí přístup k legitimním webovým zdrojům, které lze použít k poškození chráněného zařízení.
Allow access to legitimate advertisement	*(nemigruje)* Přístup k legitimní reklamě můžete spravovat pomocí kategorie webového zdroje *Bannery* v nastavení součásti Kontrola webu.
Operation mode: • **Driver Interceptor** • **Redirector** • **External Proxy**	*(nemigruje)* Kaspersky Endpoint Security podporuje pouze režim Driver Interceptor.

ICAP-service connection settings	*(nemigruje)* Kaspersky Endpoint Security nepodporuje ICAP Network Storage Protection.
Check safe connections through the HTTPS protocol	Režim **Kontrola šifrovaného připojení** / **Vždy kontrolovat šifrovaná připojení** (pododdíl **Nastavení sítě**)
Use TLS protocol version	*(nemigruje)* 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 Můžete navíc blokovat připojení SSL 2.0 v nastavení kontroly šifrovaných připojení.
Do not trust web-servers with invalid certificate	**Adresa** (pododdíl **Nastavení sítě**)
Intercept ports (Interception area)	**Sledované porty** (pododdíl **Nastavení sítě**) Během migrace KES zruší zaškrtnutí políček **Sledovat všechny porty aplikací ze seznamu doporučeného společností Kaspersky** a **Sledovat všechny porty u zadaných aplikací**.
Exclude ports (Interception area)	*(nemigruje)*
Exclude IP addresses (Interception area)	**Konfigurovat důvěryhodné adresy** (pododdíl **Nastavení sítě**)
Exclude processes (Interception area)	**Konfigurovat důvěryhodné aplikace** (pododdíl **Nastavení sítě**) Během migrace KES nakonfiguruje následující nastavení pro důvěryhodnou aplikaci: • Políčko **Nekontrolovat síťový provoz** je zaškrtnuto. KES nekontroluje síťový provoz u žádných vzdálených IP adres a žádných portů. • Ostatní zaškrtávací políčka v nastavení důvěryhodné aplikace nejsou zaškrtnuta.
Security port	*(nemigruje)*
Use malicious URL database to scan web links	**Porovnat webovou adresu s databází škodlivých webových adres** (pododdíl **Ochrana před webovými hrozbami**)
Use anti-phishing database to scan web pages	**Porovnat webovou adresu s databází phishingových webových adres** (pododdíl **Ochrana před webovými hrozbami**)
Use KSN for protection	*(nemigruje)* Kaspersky Endpoint Security používá KSN pro všechny součásti aplikace.
Use Trusted Zone	*(nemigruje)* Kaspersky Endpoint Security použije důvěryhodnou zónu na všechny součásti. Výjimky můžete nakonfigurovat v nastavení důvěryhodné zóny.
Use heuristic analyzer	**Použít heuristickou analýzu** (pododdíl **Ochrana před webovými hrozbami** a **Ochrana před hrozbami v poště**)
Security level	*(nemigruje)* Kaspersky Endpoint Security má vlastní úrovně zabezpečení pro součásti Ochrana před webovými hrozbami a Ochrana před hrozbami v poště. Ve výchozím nastavení Kaspersky Endpoint Security nastavuje doporučenou úroveň zabezpečení.
Enable mail threat protection	**Ochrana před hrozbami v poště** (pododdíl **Ochrana před hrozbami v poště**) **Připojovat rozšíření pro Microsoft Outlook** **Pouze příchozí zprávy** (Rozsah ochrany) **Kontrola během příjmu** (Ochrana e-mailu)
Schedule settings	*(nemigruje)* Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Exploit Prevention

Nastavení prevence zneužití KSWS jsou migrována do části **Rozšířená ochrana před hrozbami**, pododdílu **Prevence zneužití**.

Nastavení součásti Prevence zneužití

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Prevent vulnerable processes exploit: • **Terminate on exploit** • **Notify only**	**Při zjištění zneužití**: • **Blokovat** • **Informovat**.
Notify about abused processes via Terminal Service	*(nemigruje)* Aplikace Kaspersky Endpoint Security nepodporuje terminálové služby.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	*(nemigruje)* Kaspersky Endpoint Security neustále brání zneužití zranitelných procesů.
Protected processes	**Povolit ochranu paměti systémových procesů** Aplikace Kaspersky Endpoint Security nepodporuje výběr chráněných procesů. Můžete povolit pouze ochranu paměti systémových procesů.
Exploit prevention techniques: • **Apply all available exploit prevention techniques** • **Apply selected exploit prevention techniques**	*(nemigruje)* Kaspersky Endpoint Security používá všechny dostupné techniky prevence zneužití.

Network Threat Protection

Nastavení součásti Ochrana před síťovými hrozbami KSWS jsou migrována do části **Základní ochrana před hrozbami**, pododdílu Ochrana před síťovými hrozbami.

Nastavení Ochrany před síťovými hrozbami

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Operation mode: • **Pass-through** • **Only inform about network attacks** • **Block connections when attack is detected**	**Ochrana před síťovými hrozbami** Je-li vybrán režim **Pass-through**, součást Ochrana před síťovými hrozbami je zakázána. Je-li vybrán režim **Only inform about network attacks** nebo **Block connections when attack is detected**, součást Ochrana před síťovými hrozbami je povolena. Kaspersky Endpoint Security vždy funguje v režimu **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	*(nemigruje)* Kaspersky Endpoint Security analyzuje provoz nepřetržitě, pokud je příslušná součást povolena.
Do not control excluded IP addresses	**Výjimky**
Schedule settings	*(nemigruje)* Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Script Monitoring

Aplikace Kaspersky Endpoint Security nepodporuje součást Sledování skriptů. Sledování skriptů je řešeno jinými součástmi, např. Ochrana AMSI.

Website categories

Kaspersky Endpoint Security nepodporuje všechny kategorie aplikace Kaspersky Security for Windows Server. Kategorie, které v aplikaci Kaspersky Endpoint Security neexistují, nejsou migrovány. Pravidla klasifikace webových zdrojů s nepodporovanými kategoriemi se proto nemigrují.

Kategorie webů

Kategorie aplikace Kaspersky Security for Windows Server	Kategorie aplikace Kaspersky Endpoint Security pro systém Windows
Wargaming	Videohry
Abortion	*(nemigruje)*
Lotteries (extended)	Hry, loterie, sázky

Alcohol	Alkohol, tabák, omamné látky
Anonymous proxy servers	Anonymizéry
Anorexia	*(nemigruje)*
Rentals for real estate	*(nemigruje)*
Audio, video and software	Software, audio, video
Banks	Banky
Blogs	Blogy
Military	Zbraně, výbušniny, vojenská tematika
For children	*(nemigruje)*
Discrimination	Násilí, nesnášenlivost
Home and family	*(nemigruje)*
Hosting and domain services	Síťová komunikace
Pets and animals	*(nemigruje)*
Law and politics	Zakázáno místními zákony
Restricted by Roskomnadzor (RF)	Zakázáno zákony Ruské federace
Restricted by Federal Law 436 (RF)	Zakázáno zákony Ruské federace
Restricted by RF legislation	Zakázáno zákony Ruské federace
Restricted by global legislation	Zakázáno místními zákony
Adult dating	Obsah nevhodný pro děti
Internet services	*(nemigruje)*
Sex shops	Obsah nevhodný pro děti
Information technologies	*(nemigruje)*
Casinos, card games	Hry, loterie, sázky
Books and writing	*(nemigruje)*
Computer games	Videohry
Health and beauty	*(nemigruje)*
Culture and society	*(nemigruje)*
LGBT	Obsah nevhodný pro děti
Lotteries	Hry, loterie, sázky
Medicine	*(nemigruje)*
Fashion	*(nemigruje)*
Music	*(nemigruje)*
Drugs	Alkohol, tabák, omamné látky
Violence	Násilí, nesnášenlivost
Discontent	*(nemigruje)*
Illegal drugs	Alkohol, tabák, omamné látky
Hate and discrimination	Násilí, nesnášenlivost
Obscene vocabulary	Neuctivé, vulgární vyjadřování
Lingerie	Obsah nevhodný pro děti
News	Zpravodajská média
Nudism	Obsah nevhodný pro děti
Education	*(nemigruje)*
Online shopping	Internetoví prodejci

All communication media	Síťová komunikace
Payment by credit cards	Platební systémy
Online shopping (own payment system)	Internetoví prodejci
Online encyclopedias	*(nemigruje)*
Online banking	Banky
Weapons	Zbraně, výbušniny, vojenská tematika
Fishing and hunting	*(nemigruje)*
Payment systems	Platební systémy
Job search	Hledání práce
Search engines	*(nemigruje)*
Police decision (JP)	Zakázáno japonskou policií
Trusted by KPSN	*(nemigruje)*
Untrusted by KPSN	*(nemigruje)*
Porn	Obsah nevhodný pro děti
Media hosting and streaming	Zpravodajská média
Web Mail	Webový e-mail
Traveling	*(nemigruje)*
TV and radio	Zpravodajská média
Teasers and ads services	Bannery
Religion	Náboženství, náboženské organizace
Restaurants, cafe and food	*(nemigruje)*
Dating sites	Seznamovací servery
Sex education	Obsah nevhodný pro děti
Social networks	Sociální sítě
Sport	*(nemigruje)*
Betting	Hry, loterie, sázky
Suicide	Násilí, nesnášenlivost
Tobacco	Alkohol, tabák, omamné látky
Torrents	Torrenty
Mentioned in Federal list of extremists (RF)	Zakázáno zákony Ruské federace
File sharing	Sdílení souborů
Pharmacy	*(nemigruje)*
Hobby and entertainment	*(nemigruje)*
Chats and forums	Chaty, fóra, rychlé zprávy
Schools and universities pages	*(nemigruje)*
Astrology and esoterica	*(nemigruje)*
Extremism and racism	Násilí, nesnášenlivost
E-commerce	Internetoví prodejci
Erotic	Obsah nevhodný pro děti
Humor	*(nemigruje)*

Local activity control

Applications Launch Control

Nastavení součásti Kontrola aplikací KSWS jsou migrována do části **Kontrolní prvky zabezpečení**, pododdílu Kontrola aplikací.

Nastavení součásti Kontrola spouštění aplikací

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Operation mode: • **Statistics only** • **Active**	**Akce** (Kontrola aplikací): • **Otestovat pravidla** • **Použít pravidla**.
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nemigruje)* Kaspersky Endpoint Security kontroluje aplikaci pokaždé, když se pokusí spustit.
Deny the command interpreters launch with no command to execute	*(nemigruje)* Aplikace Kaspersky Endpoint Security umožňuje spouštění překladačů příkazů, pokud nejsou zakázány součástí Kontrola aplikací.
Rules	**Pravidla součásti Kontrola aplikací** *(podporováno s omezeními)* Kaspersky Endpoint Security 11.11.0 zavádí podporu pro migraci pravidel součásti Kontrola spouštění aplikací. Funkce migrace pravidel součásti Kontrola spouštění aplikací má některá omezení. Standardně Kontrola spouštění aplikací KSWS zahrnuje dvě pravidla: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** Pokud je alespoň jedno zdrojové pravidlo KSWS typu **Allow**, během migrace vytvoří aplikace KES nové povolující pravidlo, **Applications with trusted root certificates**. To znamená, že nástroj součást Kontrola aplikací KES používá pro povolení spouštění důvěryhodných skriptů, balíčků MSI a spustitelných souborů jedno pravidlo. Pokud jsou obě zdrojová pravidla KSWS typu **Deny**, KES nepřidává pravidla pro správu aplikací s důvěryhodnými kořenovými certifikáty.
Apply rules to executable files	*(nemigruje)* Rozsah aplikace pravidla nelze nakonfigurovat v nastavení součásti Kontrola aplikací KES. Kontrola aplikací KES uplatňuje pravidla na všechny typy souborů: spustitelné soubory, skripty a balíčky MSI. Pokud jsou všechny typy souborů zahrnuty do rozsahu použití pravidel v KSWS, KES během migrace tato pravidla KSWS přenese. Pokud je některý typ souboru vyloučen z rozsahu použití pravidel v KSWS, KES během migrace přenese také pravidla KSWS, ale jako akce součásti Kontrola aplikací je vybrána možnost **Otestovat pravidla**.
Monitor loading of DLL modules	**Monitorovat zavádění modulů DLL (výrazně zvýší zatížení systému)**
Apply rules to scripts and MSI packages	*(nemigruje)* Rozsah aplikace pravidla nelze nakonfigurovat v nastavení součásti Kontrola aplikací KES. Kontrola aplikací KES uplatňuje pravidla na všechny typy souborů: spustitelné soubory, skripty a balíčky MSI. Pokud jsou všechny typy souborů zahrnuty do rozsahu použití pravidel v KSWS, KES během migrace tato pravidla KSWS přenese. Pokud je některý typ souboru vyloučen z rozsahu použití pravidel v KSWS, KES během migrace přenese pravidla KSWS, ale jako akce součásti Kontrola aplikací je vybrána možnost **Otestovat pravidla**.
Deny applications untrusted by KSN	*(nemigruje)* Kaspersky Endpoint Security nebere v úvahu reputaci aplikací a povoluje nebo zakazuje spouštění aplikací v souladu s pravidly.
Allow applications trusted by KSN	Během migrace KES přidá nové povolující pravidlo. Jako podmínka spuštění pravidla je zadána kategorie KL **Ostatní software\Aplikace, důvěryhodné podle reputace v KSN**.
Users and / or user groups allowed to run applications trusted by KSN	**Uživatelé a jejich práva** v povolujícím pravidle součásti Kontrola aplikací, které zahrnuje kategorii KL **Ostatní software\Aplikace, důvěryhodné podle reputace v KSN**.
Automatically allow software distribution via applications and packages listed	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru. Jako podmínka aktivace pravidla je zadán hash souboru.
Always allow software distribution via Windows Installer	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru (**Software distribution applications and packages allowed**). Jako podmínka aktivace pravidla je zadán hash souboru. Ve vlastnostech účtu je zaškrtnuto políčko **Důvěryhodné nástroje aktualizace**.

Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nemigruje)*
Software distribution applications and packages allowed	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru. Jako podmínka aktivace pravidla je zadán hash souboru. Ve vlastnostech účtu je zaškrtnuto políčko **Důvěryhodné nástroje aktualizace**.
Schedule settings	*(nemigruje)* Pokud je pro součást v nastavení KSWS nakonfigurován plán, je součást Kontrola aplikací při migraci povolena. Jestliže pro součást v nastavení KSWS není nakonfigurován plán, je součást Kontrola aplikací při migraci zakázána. Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Device Control

Nastavení součásti Kontrola zařízení KSWS jsou migrována do části **Kontrolní prvky zabezpečení**, pododdílu **Kontrola zařízení**.

Nastavení součásti Kontrola zařízení

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Operation mode: • **Active** • **Statistics only**	*(nemigruje)* Kontrola aplikací funguje v režimu *Active*. Statistiky připojení zařízení průběžně poskytuje audit.
Allow using all external devices when the Device Control task is not running	*(nemigruje)* Kontrola zařízení je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.
Device Control rules	**Důvěryhodná zařízení** Během migrace aplikace Kaspersky Endpoint Security ignoruje zakázaná pravidla KSWS.
Schedule settings	*(nemigruje)* Kaspersky Endpoint Security používá vlastní plán pro získání přístupu k určitým typům zařízení.

Network-Attached Storages Protection

RPC Network Storage Protection

Kaspersky Endpoint Security nepodporuje součásti Ochrana síťově připojených úložišť. Pokud tyto součásti potřebujete, můžete pokračovat v používání aplikace Kaspersky Security for Windows Server.

ICAP Network Storage Protection

Kaspersky Endpoint Security nepodporuje součásti Ochrana síťově připojených úložišť. Pokud tyto součásti potřebujete, můžete pokračovat v používání aplikace Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

Kaspersky Endpoint Security nepodporuje Anti-Cryptor pro NetApp. Funkci Anti-Cryptor zajišťují další součásti aplikace, např. Detekce chování.

Network activity control

Firewall Management

Aplikace Kaspersky Endpoint Security nepodporuje správu brány firewall KSWS. Funkce brány firewall KSWS provádí systémová brána firewall. Po migraci můžete nakonfigurovat bránu firewall aplikace Kaspersky Endpoint Security.

Anti-Cryptor

Síťová nastavení funkce Anti-Cryptor jsou migrována do části **Rozšířená ochrana před hrozbami**, pododdílu **Detekce chování**.

Nastavení funkce Anti-Cryptor

Nastavení KSWS	Nastavení KES
Operation mode: • **Statistics only** • **Active**	**Při zjištění externího šifrování sdílených složek**: • **Informovat** • **Blokovat**.
Heuristic analyzer	*(nemigruje)* Kaspersky Endpoint Security nepoužívá heuristickou analýzu pro detekci chování.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	*(nemigruje)* Kaspersky Endpoint Security zabraňuje šifrování všech sdílených síťových složek chráněného počítače.
Exclusions	*(nemigruje)* Aplikace Kaspersky Endpoint Security má vlastní výjimky pro součást Detekce chování. Výjimky můžete přidat ručně po migraci.
Schedule settings	*(nemigruje)* Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

System Inspection

File Integrity Monitor

Nastavení funkce Monitor integrity souborů z KSWS jsou migrována do části **Kontrolní prvky zabezpečení**, pododdílu **Monitorování integrity systému**.

Nastavení funkce Monitor integrity souborů

Nastavení KSWS	Nastavení KES
Log information about file operations that appear during the monitor interruption period	*(nemigruje)* Kaspersky Endpoint Security nezaznamenává do protokolu události u operací se soubory prováděných během doby přerušení monitoru.
Block attempts to compromise the USN log	*(nemigruje)* Kaspersky Endpoint Security neblokuje pokusy o narušení protokolu USN.
Monitoring scope	**Rozsah monitorování** → **Soubor** *(podporováno s omezeními)* Zakázané záznamy rozsahu monitorování se nemigrují do KES. Kaspersky Endpoint Security přidá do rozsahu monitorování pouze povolené záznamy.
Trusted users	**Důvěryhodní uživatelé a/nebo skupiny uživatelů**
File operation markers	**Deskriptory operace se souborem**
Calculate checksum for the file if possible	**Hashování**
Exclusions	**Výjimky** → **Soubor**

Log Inspection

Nastavení součásti Kontrola protokolu KSWS jsou migrována do části **Kontrolní prvky zabezpečení**, pododdílu **Kontrola protokolu**.

Nastavení kontroly protokolu

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Apply custom rules for log inspection	*(nemigruje)* Kaspersky Endpoint Security uplatní všechna povolená vlastní pravidla.
Custom rules	**Vlastní pravidla** Předdefinované pravidlo **A service was installed in the system (for Server 2003 OS)** není migrováno do KES.
Apply predefined rules for log inspection	*(nemigruje)* Kaspersky Endpoint Security uplatní všechna povolená předdefinovaná pravidla.
Predefined rules	**Předdefinovaná pravidla**
Password brute-force detection	**Zjišťování útoku hrubou silou**
Network logon detection	**Detekce přihlášení k síti**
Exclusions (IP addresses)	**Výjimky** (IP adresa)
Exclusions (users)	**Výjimky** (Uživatelé)
Schedule settings	*(nemigruje)* Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Logs and notifications

Task logs

Nastavení protokolů KSWS jsou migrována do části **Obecná nastavení**, pododdílů Rozhraní a Zprávy a úložiště.

Nastavení protokolů

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Event logging	**Upozornění** (pododdíl **Rozhraní**)
Logs folder	*(nemigruje)* Aplikace Kaspersky Endpoint Security ukládá zprávy do složky `C:\ProgramData\Kaspersky Lab\KES.14.0\Report`.
Remove task logs older than N day(s)	*(nemigruje)* Dobu uchovávání zpráv KES můžete nakonfigurovat v části **Obecná nastavení**, **Zprávy a úložiště**.
Remove from the audit log events N day(s)	*(nemigruje)* Kaspersky Endpoint Security uplatňuje omezení úložiště zpráv na všechny zprávy včetně zpráv o auditu systému.
Integration with SIEM	*(nemigruje)* Integraci se SIEM můžete nakonfigurovat v aplikaci Kaspersky Security Center.

Event notifications

Nastavení upozornění KSWS jsou migrována do části **Obecná nastavení**, pododdílu Rozhraní.

Nastavení upozornění

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Notifications	**Upozornění**
Notify users: • **By using terminal service** • **By using Windows Messenger Service command**	*(nemigruje)* Aplikace Kaspersky Endpoint Security nepodporuje úpravu textu upozornění. Aplikace Kaspersky Endpoint Security zobrazuje standardní oznámení.

Notify administrators: • **By using Windows Messenger Service command** • **By running executable file** • **By sending email**	Do Kaspersky Endpoint Security jsou migrována pouze nastavení upozornění e-mailem – **Nastavení upozornění e-mailem** (skupina **Upozornění**). Jiné způsoby upozornění správců nejsou podporovány.
Application database is out of date	**V případě, že databáze nebyly aktualizovány, odeslat upozornění "Databáze nejsou aktuální"**
Application database is extremely out of date	**V případě, že databáze nebyly aktualizovány, odeslat upozornění "Databáze jsou výrazně zastaralé"**
Critical areas scan has not been performed for a long time	*(nemigruje)* Kaspersky Endpoint Security generuje zmeškanou událost kontroly kritických oblastí po třech dnech.

Interaction with Administration Server

Nastavení interakce se serverem pro správu KSWS jsou migrována do části **Obecná nastavení**, pododdílu **Zprávy a úložiště**.

Nastavení interakce se serverem pro správu

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Quarantined files	**Soubory v karanténě**
Backed up files	**Soubory zálohy**
Blocked hosts	*(nemigruje)* Kaspersky Endpoint Security automaticky odesílá data o blokovaných hostitelích.

Tasks

Activating the application

Aplikace Kaspersky Endpoint Security nepodporuje úlohu *Application activation* (KSWS). Můžete vytvořit a přidat úlohu *Přidání klíče* (KES), přidat licenční klíč do instalačního balíčku nebo povolit automatickou distribuci licenčního klíče.

Copying Updates

Nastavení úlohy *Copying Updates* (KSWS) se migrují do úlohy *Aktualizace databází a modulů aplikace* (KES).

Nastavení úlohy Aktualizace

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Aktualizační zdroj**: • **Kaspersky Security Center** • **Aktualizační servery společnosti Kaspersky** • **Zadáno uživatelem**.
Use Kaspersky update servers if specified servers are not available	*(nemigruje)* Kaspersky Endpoint Security umožňuje výběr více zdrojů aktualizací, včetně aktualizačních serverů Kaspersky. Pokud není první zdroj aktualizací dostupný, Kaspersky Endpoint Security vám umožní získat aktualizace z jiného zdroje v seznamu.
Use proxy server settings to connect to Kaspersky update servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.
Use proxy server settings to connect to other servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.

Copying updates settings: • **Copy database updates** • **Copy critical software modules updates** • **Copy database updates and critical updates of application modules**	*(nemigruje)* Kaspersky Endpoint Security kopíruje aktualizace databáze a kritické aktualizace modulů aplikace jako jeden balíček.
Folder for local storage of copied updates	**Zkopírovat aktualizace do složky**

Baseline File Integrity Monitor

Nastavení úlohy *Baseline File Integrity Monitor* (KSWS) se migrují do úlohy *Kontrola integrity systému* a do části zásady **Kontrolní prvky zabezpečení**, pododdílu **Monitorování integrity systému**.

Nastavení úlohy Monitorování integrity souborů v porovnání se základním stavem

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Hash calculation algorithm: • **MD5**. • **SHA256**.	*(nemigruje)* Kaspersky Endpoint Security používá pro výpočet kontrolního součtu algoritmus SHA256.
Scan scope	**Rozsah monitorování** (pododdíl **Monitorování integrity systému**)

Database Update

Nastavení úlohy *Database Update* (KSWS) se migrují do úlohy *Aktualizace databází a modulů aplikace* (KES).

Nastavení úlohy Aktualizace databáze

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Aktualizační zdroj**: • **Kaspersky Security Center** • **Aktualizační servery společnosti Kaspersky** • **Zadáno uživatelem**.
Use Kaspersky update servers if specified servers are not available	*(nemigruje)* Kaspersky Endpoint Security umožňuje výběr více zdrojů aktualizací, včetně aktualizačních serverů Kaspersky. Pokud není první zdroj aktualizací dostupný, Kaspersky Endpoint Security vám umožní získat aktualizace z jiného zdroje v seznamu.
Use proxy server settings to connect to Kaspersky update servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.
Use proxy server settings to connect to other servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.
Lower the load on the disk I/O	*(nemigruje)*

Software modules updates

Nastavení úlohy *Software Modules Update* (KSWS) se migrují do úlohy *Aktualizace databází a modulů aplikace* (KES).

Nastavení úlohy Aktualizace softwarových modulů

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

Update source: • **Kaspersky Security Center Administration Server** • **Kaspersky update servers** • **Custom HTTP or FTP servers, or network folders**	**Aktualizační zdroj**: • **Kaspersky Security Center** • **Aktualizační servery společnosti Kaspersky** • **Zadáno uživatelem**.
Use Kaspersky update servers if specified servers are not available	*(nemigruje)* Kaspersky Endpoint Security umožňuje výběr více zdrojů aktualizací, včetně aktualizačních serverů Kaspersky. Pokud není první zdroj aktualizací dostupný, Kaspersky Endpoint Security vám umožní získat aktualizace z jiného zdroje v seznamu.
Use proxy server settings to connect to Kaspersky update servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.
Use proxy server settings to connect to other servers	*(nemigruje)* Kaspersky Endpoint Security používá proxy server pro všechny součásti. Můžete nakonfigurovat připojení k proxy serveru v síťových možnostech aplikace.
Copy and install critical software modules updates	**Instalovat důležité a schválené aktualizace**
Only check for critical software updates available	*(nemigruje)* Kaspersky Endpoint Security neustále kontroluje dostupnost kritických aktualizací modulů aplikace.
Allow operating system restart	*(nemigruje)* Kaspersky Endpoint Security vyzve uživatele k povolení restartování počítače.
Receive information about available scheduled software modules updates	*(nemigruje)* Kaspersky Endpoint Security zobrazí upozornění na aktualizace softwarových modulů.

Rollback of Application Database Update

Nastavení úlohy *Rollback of Application Database Update* (KSWS) se migrují do úlohy *Vrácení aktualizace zpět* (KES). Nová úloha *Vrácení aktualizace zpět* (KES) má plán spouštění úlohy *Manually*.

On-Demand Scan

Nastavení úlohy *On-Demand Scan* (KSWS) se migrují do úlohy *Kontrola malwaru* (KES).

Nastavení úlohy Antivirová kontrola

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Scan scope	**Rozsah kontroly**
Protection level: • **Maximum protection** • **Recommended** • **Maximum performance**	**Úroveň zabezpečení**: • **Vysoká** • **Doporučená** • **Nízká**. Nastavení úrovně zabezpečení se v KSWS a KES liší.
Objects to scan: • **All objects** • **Objects scanned by format** • **Objects scanned according to list of extensions specified in anti-virus database** • **Objects scanned by specified list of extensions**	**Typy souborů**: • **Všechny soubory** • **Soubory podle formátu** • **Soubory podle přípony**. Kaspersky Endpoint Security neumožňuje vytváření vlastních seznamů rozšíření. Kaspersky Endpoint Security nahradí hodnotu **Objects scanned by specified list of extensions** hodnotou **Soubory podle přípony**.
Subfolders	**Včetně podsložek**
Subfiles	*(nemigruje)*

Scan disk boot sectors and MBR	*(nemigruje)*
Scan alternate NTFS streams	*(nemigruje)*
Scan only new and modified files	**Kontrolovat pouze nové a upravené soubory**
Scan of compound objects:	**Kontrola složených souborů**:
• **All archives** • **All SFX archives** • **All email databases** • **All packed objects** • **All plain email** • **All embedded OLE objects**	• **Kontrolovat archivy** • **Kontrolovat archivy chráněné heslem** • **Kontrolovat distribuční balíčky** • **Kontrolovat soubory v poštovním formátu** • **Kontrolovat soubory ve formátu aplikací Microsoft Office**.
Action to perform on infected and other objects:	**Akce při zjištění hrozby**:
• **Disinfect** • **Disinfect. Remove if disinfection fails** • **Remove** • **Perform recommended action** • **Notify only**	• **Dezinfikovat; a pokud se dezinfekce nezdaří, tak odstranit** • **Dezinfikovat; a pokud se dezinfekce nezdaří, tak informovat** • **Informovat**.
Action to perform on probably infected objects: • **Quarantine** • **Remove** • **Perform recommended action** • **Notify only**	*(nemigruje)* Kaspersky Endpoint Security provede akci, pokud je zjištěna jakákoliv hrozba.
Perform actions depending on the type of object detected	*(nemigruje)*
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	*(nemigruje)*
Exclude files	*(nemigruje)* Kaspersky Endpoint Security použije důvěryhodnou zónu na všechny součásti. Výjimky můžete nakonfigurovat v nastavení důvěryhodné zóny.
Do not detect	*(nemigruje)*
Stop scanning if it takes longer than N sec	**Přeskočit soubory, které se kontrolují déle než N s**
Do not scan compound objects larger than N MB	**Nerozbalovat velké složené soubory**
Use iSwift technology	**Technologie iSwift**
Use iChecker technology	**Technologie iChecker**
Action on the offline files: • **Do not scan** • **Scan resident part of file only** • **Scan entire file** • **Only if the file has been accessed within the specified period (days)** • **Do not copy file to a local hard drive, if possible**	*(nemigruje)* Kaspersky Endpoint Security kontroluje offline soubory jako celek.

Application Integrity Check

Nastavení úlohy *Application Integrity Control* (KSWS) se migrují do úlohy *Kontrola integrity aplikací* (KES).

Rule Generator for Applications Launch Control

Aplikace Kaspersky Endpoint Security nepodporuje úlohu *Applications Launch Control Generator*. Pravidla můžete generovat v nastavení součásti Kontrola aplikací.

Rule Generator for Device Control

Aplikace Kaspersky Endpoint Security nepodporuje úlohu *Rule Generator for Device Control*. Pravidla přístupu můžete generovat v nastavení součásti Kontrola zařízení.

Migrace součástí KSWS

Aplikace Kaspersky Endpoint Security před místní instalací zkontroluje přítomnost aplikací společnosti Kaspersky v počítači. Pokud je na počítači nainstalována aplikace Kaspersky Security for Windows Server, KES detekuje sadu součástí KSWS, které jsou nainstalovány, a vybere stejné součásti k instalaci.

Součásti KES, které KSWS nemá, se instalují následovně:

- Ochrana AMSI, Prevence narušení hostitele, Modul pro nápravu se instalují s výchozím nastavením.
- Součásti Ochrana před útoky BadUSB, Adaptivní kontrola anomálií, Šifrování dat, Detection and Response jsou ignorovány.

Při vzdálené instalaci aplikace KES ignoruje sadu nainstalovaných součástí KSWS. Instalační program nainstaluje součásti, které vyberete ve vlastnostech instalačního balíčku. Po instalaci aplikace Kaspersky Endpoint Security a migraci zásad a úloh se nastavení KES konfigurují v souladu s nastavením KSWS.

Migrace úloh a zásad KSWS

Nastavení zásad a úloh KSWS lze migrovat následujícími způsoby:

- Použití průvodce hromadným převodem zásad a úloh (dále také označovaný jako „průvodce migrací").

  Průvodce migrací pro KSWS je k dispozici pouze v konzole pro správu (MMC). Nastavení zásad a úloh nelze migrovat ve webové konzole a cloudové konzole.

  Průvodce hromadným převodem funguje odlišně pro různé verze aplikace Kaspersky Security Center. Doporučujeme upgradovat řešení na verzi 14.2 nebo vyšší. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh umožňuje migrovat zásady do profilu, nikoli do zásady. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh také umožňuje migrovat širší rozsah nastavení zásad.

- Používání průvodce novou zásadou pro aplikaci Kaspersky Endpoint Security pro systém Windows.

  Průvodce novou zásadou vám umožňuje vytvořit zásadu KES na základě zásady KSWS.

Postupy migrace zásad KSWS se liší při použití průvodce migrací a průvodce novou zásadou.

Průvodce hromadným převodem zásad a úloh

Průvodce migrací přenese nastavení zásad KSWS do profilu zásad namísto nastavení zásad KES. *Profil zásad* je sada nastavení zásad, která se v počítači aktivuje, pokud počítač splňuje nakonfigurovaná aktivační pravidla. Jako aktivační kritérium profilu zásad je vybrána značka zařízení `UpgradedFromKSWS`. Kaspersky Security Center automaticky přidá značku `UpgradedFromKSWS` ke všem počítačům, na které instalujete KES přes KSWS pomocí úlohy vzdálené instalace. Pokud jste zvolili jiný způsob instalace, můžete značku přiřadit zařízením ručně.

Přidání značky k zařízení:

1. Vytvoření nové značky pro servery – `UpgradedFromKSWS`.

   Podrobnosti o vytváření značek pro zařízení najdete v nápovědě k aplikaci Kaspersky Security Center.

2. V konzole aplikace Kaspersky Security Center vytvořte novou skupinu správy a přidejte do ní servery, kterým chcete přiřadit značku.

   Servery můžete seskupit pomocí nástroje pro výběr. Podrobnosti o práci s výběry najdete v nápovědě k aplikaci Kaspersky Security Center.

3. V konzole aplikace Kaspersky Security Center vyberte všechny servery příslušné skupiny správy, otevřete vlastnosti vybraných serverů a přiřaďte značku.

Pokud migrujete více zásad KSWS, každá zásada se převede do profilu v rámci jedné zastřešující zásady. Pokud zásada KSWS již obsahuje profily, budou tyto profily také migrovány jako profily. Získáte tak jednu zásadu, která obsahuje profily odpovídající všem zásadám KSWS.

Jak pomocí průvodce hromadným převodem zásad a úloh migrovat nastavení zásad KSWS

1. V konzole pro správu vyberte položku Administration Server a kliknutím pravým tlačítkem otevřete místní nabídku.

2. Vyberte **All tasks → Policies and tasks batch conversion wizard**.

Spustí se průvodce hromadným převodem zásad a úloh. Postupujte podle pokynů průvodce.

Krok 1. Výběr aplikace, pro kterou potřebujete převést zásady a úlohy

V tomto kroku musíte vybrat Kaspersky Endpoint Security pro systém Windows. Přejděte k dalšímu kroku.

Krok 2. Převod zásad

Průvodce migrací vytvoří profily zásad KSWS uvnitř zásady KES. Vyberte zásady aplikace Kaspersky Security for Windows Server, které chcete převést do profilů zásad. Přejděte k dalšímu kroku.

Průvodce migrací poté začne převádět zásady. Názvy nových profilů zásad budou odpovídat původním zásadám KSWS.

Krok 3. Zpráva o migraci zásad

Průvodce migrací vytvoří zprávu o migraci zásad. Zpráva o migraci zásad obsahuje datum a čas, kdy byly zásady převedeny, název původní zásady KSWS, název cílové zásady KES a název nového profilu zásad.

Krok 4. Převod úloh

Nové úlohy pro aplikaci Kaspersky Endpoint Security pro systém Windows vytvoří průvodce migrací. V seznamu úloh vyberte úlohy aplikace KSWS, které chcete vytvořit pro zásady aplikace Kaspersky Endpoint Security. Nové úlohy budou mít název *<Název úlohy KSWS> (converted)*. Přejděte k dalšímu kroku.

Krok 5. Dokončení průvodce

Ukončete průvodce. Průvodce tak provede následující:

- Do zásad Kaspersky Endpoint Security jsou přidány nové profily zásad.

  Zásady zahrnují profily s nastavením aplikace Kaspersky Security for Windows Server. Nová zásada má stav *Active*. Průvodce ponechá zásady KSWS beze změny.

- Vytvoří nové úlohy aplikace Kaspersky Endpoint Security.

  Nové úlohy jsou kopiemi úloh KSWS. Průvodce ponechá úlohy KSWS beze změny.

Nový profil zásad s nastavením KSWS bude pojmenován *UpgradedFromKSWS<název zásady aplikace Kaspersky Security for Windows Server>*. Ve vlastnostech profilu průvodce migrací automaticky vybere jako aktivační kritérium značku `UpgradedFromKSWS`. Nastavení z profilu zásad se tedy na servery aplikují automaticky.

Průvodce vytvořením zásady založené na zásadě KSWS

Když je zásada KES vytvořena na základě zásady KSWS, průvodce podle toho přenese nastavení do nové zásady. To znamená, že jedna zásada KES bude odpovídat jedné zásadě KSWS. Průvodce nepřevede zásadu na profil.

Jak pomocí průvodce novou zásadou migrovat nastavení zásady KSWS

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 zásadami.

Krok 1. Výběr aplikace pro vytvoření zásady skupiny

Vyberte aplikaci **Kaspersky Endpoint Security for Windows (14.0)**.

Krok 2. Pojmenování zásady skupiny

Zadejte název zásady skupiny, například *Zásady pro kancelář*.

Zaškrtněte políčko **Use policy settings for an earlier version of the application**. Klikněte **Browse** a vyberte zásadu KSWS.

Krok 3. Účast ve službě Kaspersky Security Network

Přečtěte si a přijměte podmínky Prohlášení o Kaspersky Security Network (KSN).

Krok 4. Výběr režimu používání aplikace v počítačích

Vyberte možnost **Standardní režim na ochranu hostitelů**. Kaspersky Endpoint Security poskytuje společné zásady pro všechny režimy aplikace a typy OS.

Pro různé režimy a typy operačního systému doporučujeme používat různé zásady.

Krok 5. Import nastavení

Tento krok je k dispozici, pokud v kroku 4 vyberete ruční konfiguraci zásad.

Zásady můžete vytvořit na základě nastavení aplikace Kaspersky Endpoint Security z konfiguračního souboru CFG. Při importu konfiguračního souboru aplikace nemusí mít průvodce k dispozici všechna nastavení zásad. V nastavení aplikace chybí například profily zásad. Pokud chcete do zásad přenést všechna nastavení a profily, můžete importovat jinou zásadu ze souboru KLP.

Při importu konfiguračního souboru aplikace Kaspersky Endpoint Security nepřenáší hesla ke kryptokontejnerům. Pokud při připojování k serverům používáte obousměrné ověřování, musíte úplně zadávat hesla ke kryptokontejnerům ručně.

Krok 6–10. Konfigurace nastavení zásad

Tento krok je k dispozici, pokud v kroku 4 vyberete ruční konfiguraci zásad.

Postupujte podle pokynů pro správu nastavení zásad.

Krok 11. Konfigurace důvěryhodné zóny

Nakonfigurujte důvěryhodnou zónu. Můžete přidat předdefinované výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou také pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security v režimu Light Agent ve virtuálních prostředích Citrix a VMware.

Krok 12. Výběr stavu zásady

- **Active**. Po další synchronizaci bude zásada v počítači použita jako aktivní zásada.

  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.

- **Inactive**. Slouží jako záložní zásada. V případě potřeby lze neaktivní zásadu přepnout do aktivního stavu.

  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.

- **Out-of-office**. Zásada je aktivována v případě, že počítač opustí hranice sítě organizace.

Ukončete průvodce.

Dodatečná konfigurace zásad a úkolů po migraci

KSWS a KES mají různé sady součást a nastavení zásad, takže po migraci musíte ověřit, že nastavení zásad splňují bezpečnostní požadavky vašeho podniku.

Zkontrolujte následující základní nastavení zásad:

- Ochrana heslem. Nastavení ochrany heslem KSWS se nemigrují. Kaspersky Endpoint Security má integrovanou funkci ochrany heslem. Pokud je třeba, zapněte ochranu heslem a nastavte heslo.
- Důvěryhodná zóna. Metody používané aplikacemi KSWS a KES pro výběr objektů se liší. Při migraci KES podporuje výjimky definované jako jednotlivé soubory nebo cesty k souboru/složce. Pokud má KSWS výjimky nakonfigurované jako předdefinovaná oblast nebo adresa URL skriptu, tyto výjimky se nemigrují. Po migraci musíte tyto výjimky přidat ručně.

  Abyste se ujistili, že aplikace Kaspersky Endpoint Security na serverech funguje správně, doporučujeme přidat soubory důležité pro fungování serveru do důvěryhodné zóny. U serverů SQL musíte přidat databázové soubory MDF a LDF. U serverů Microsoft Exchange musíte přidat soubory CHK, EDB, JRS, LOG a JSL. Můžete použít masky, např. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

- Brána firewall. Funkce brány firewall KSWS provádí systémová brána firewall. V KES je za funkčnost brány firewall zodpovědná samostatná součást. Po migraci můžete nakonfigurovat bránu firewall aplikace Kaspersky Endpoint Security.
- Služba Kaspersky Security Network Kaspersky Endpoint Security nepodporuje konfiguraci KSN pro jednotlivé součásti. Kaspersky Endpoint Security používá KSN pro všechny součásti aplikace. Chcete-li používat KSN, musíte přijmout nové podmínky Prohlášení o Kaspersky Security Network.
- Kontrola webu Pravidla blokování pro řízení kategorií webového provozu jsou v aplikaci Kaspersky Endpoint Security migrována do jediného pravidla blokování. Kaspersky Endpoint Security ignoruje povolená pravidla pro řízení kategorií. Kaspersky Endpoint Security nepodporuje všechny kategorie aplikace Kaspersky Security for Windows Server. Kategorie, které v aplikaci Kaspersky Endpoint Security neexistují, nejsou migrovány. Pravidla klasifikace webových zdrojů s nepodporovanými kategoriemi se proto nemigrují. Pokud je třeba, přidejte pravidla součásti Kontrola webu.
- Proxy servery. Heslo pro připojení k proxy serveru se nemigruje. Ručně zadejte heslo, které se použije pro připojení k proxy serveru.
- Plány jednotlivých součástí. Kaspersky Endpoint Security nepodporuje konfiguraci plánů pro jednotlivé součásti. Součásti jsou vždy zapnuté, když je aplikace Kaspersky Endpoint Security v provozu.
- Sada součástí. Sada dostupných funkcí aplikace Kaspersky Endpoint Security závisí na typu operačního systému: pracovní stanice, nebo server. Například z nástrojů pro šifrování je na serverech k dispozici pouze nástroj BitLocker Drive Encryption.
- Atribut . Stav atributu se nemigruje. Atribut bude mít výchozí hodnotu. Ve výchozím nastavení mají téměř všechna nastavení v nové zásadě zákaz upravovat nastavení v podřízených zásadách a v místním rozhraní aplikace. Atribut hodnotu pro nastavení zásad v části **Managed Detection and Response (Industrial CyberSecurity)** a ve skupině nastavení **Uživatelská podpora** skupina nastavení (část **Rozhraní**). V případě potřeby nakonfigurujte dědění nastavení z nadřazené zásady.
- Práce s aktivními hrozbami. Pokročilá dezinfekce funguje jinak u pracovních stanic a serverů. Pokročilou dezinfekci můžete nakonfigurovat v nastavení úlohy *Kontrola malwaru* a v nastavení aplikace.
- Upgrade aplikace. Chcete-li nainstalovat hlavní aktualizace a opravy bez restartování, musíte změnit režim aktualizace aplikace. Ve výchozím nastavení je funkce Nainstalovat aktualizace aplikace bez restartování počítače zakázána.
- Kaspersky Endpoint Agent. Kaspersky Endpoint Security má integrovaného agenta pro práci s řešeními Detection and Response. Pokud je třeba, přeneste nastavení zásad aplikace Kaspersky Endpoint Agent do zásad aplikace Kaspersky Endpoint Security.
- Úlohy *Aktualizace databází a modulů aplikace*. Ujistěte se, že byla nastavení úlohy *Aktualizace databází a modulů aplikace* úlohy migrována správně. Místo tří úloh KSWS používá KES jedinou úlohu KES. Můžete optimalizovat úlohu *Aktualizace databází a modulů aplikace* a odstranit nadbytečné úlohy.
- Další úlohy. Součásti Kontrola aplikací, Kontrola zařízení a Monitor integrity souborů fungují v KSWS a KES odlišně. KES nepoužívá úlohy *Baseline File Integrity Monitor*, *Applications Launch Control Generator* a *Rule Generator for Device Control*. Tyto úlohy proto nejsou migrovány. Po migraci můžete nakonfigurovat součásti Monitor integrity souborů, Kontrola aplikací a Kontrola zařízení.

Migrace důvěryhodné zóny KSWS

Důvěryhodná zóna je správcem konfigurovaný seznam objektů a aplikací, které aplikace Kaspersky Endpoint Security nesleduje, když jsou aktivní. Objekty důvěryhodné zóny můžete migrovat z KSWS do KES pomocí *průvodce hromadným převodem zásad a úloh* nebo *průvodce vytvořením nové zásady KES založené na zásadě KSWS*. KSWS a KES mají různé sady součástí a funkcí, takže po migraci musíte ověřit, že výjimky splňují bezpečnostní požadavky vašeho podniku. Mezi KES a KSWS se liší i metody přidávání výjimek do důvěryhodné zóny. Průvodce migrací nemá nástroje na migraci všech výjimek KSWS. To znamená, že po migraci musíte některé výjimky KSWS přidat ručně.

Abyste se ujistili, že aplikace Kaspersky Endpoint Security na serverech funguje správně, doporučujeme přidat soubory důležité pro fungování serveru do důvěryhodné zóny. U serverů SQL musíte přidat databázové soubory MDF a LDF. U serverů Microsoft Exchange musíte přidat soubory CHK, EDB, JRS, LOG a JSL. Můžete použít masky, např. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

Metody vytvoření důvěryhodné zóny KES a KSWS.

KSWS		KES
Object to scan		
• Predefined scope	*(nemigruje)*	
• Disk, folder or network location	→	**Soubor nebo složka**
• File	→	**Soubor nebo složka**
• Script file or web address	*(nemigruje)*	
Detected object	→	**Typ zjištěného objektu**
Trusted processes	→	**Důvěryhodné aplikace**

Migrace kontrolovaných objektů

Výjimky KSWS, které mají ve vlastnostech vybranou metodu **Object to scan**, se migrují do výjimek KES, které mají ve vlastnostech vybránu metodu **Soubor nebo složka** (s některými omezeními). Migrace výjimky závisí na metodě výběru objektu:

- Predefined scope – *nemigruje se*.

  Po migraci musíte tyto výjimky přidat ručně. Výjimky a předdefinované oblasti je nutno nakonfigurovat v nastavení úlohy *Kontrola malwaru*.

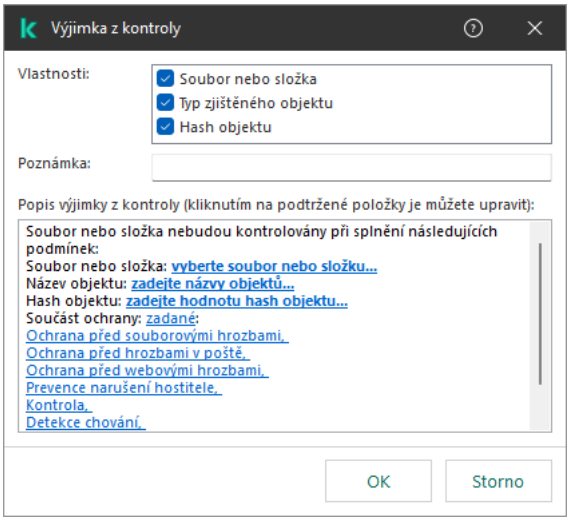
- Disk, folder or network location – migrace na výjimky KES, které mají ve vlastnostech vybránu metodu „Soubor nebo složka".

- File – migrace na výjimky KES, které mají ve vlastnostech vybránu metodu „Soubor nebo složka".

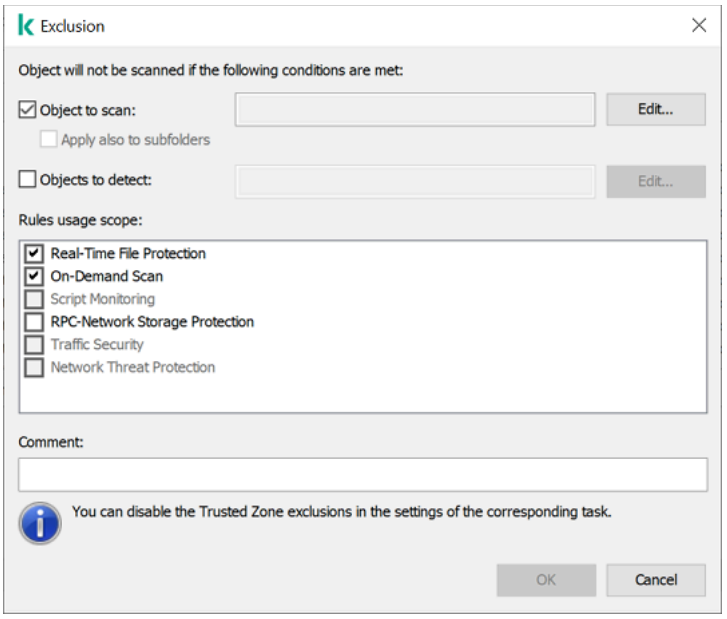
- Script file or web address – *nemigruje se*.

  Po migraci musíte tyto výjimky přidat ručně. Výjimky jako webové adresy skriptů musíte přidat k důvěryhodným webovým adresám součásti Ochrana před webovými hrozbami.

Je-li u kontrolovaného objektu zaškrtnuto políčko **Apply also to subfolders**, toto nastavení se migruje do výjimek KES (políčko **Včetně podsložek**).



Nastavení výjimek KES



Nastavení výjimek KSWS

Migrace zjištěných objektů

Výjimky KSWS, které mají ve vlastnostech vybranou metodu **Detected object**, se migrují do výjimek KES, které mají ve vlastnostech vybránu metodu **Typ zjištěného objektu**. Název zjištěného objektu odpovídá klasifikaci encyklopedie Kaspersky (například `Email-Worm`, `Rootkit` nebo `RemoteAdmin`). Kaspersky Endpoint Security podporuje masky s otazníkem `?` (za jakýkoli jeden znak) a hvězdičkou `*` (za jakoukoli sekvenci znaků).

Migrace rozsahu použití výjimky

Rozsah použití výjimky je sada součástí, na které se výjimka uplatňuje. KES a KSWS mají odlišné sady součástí, takže průvodce migrací nemůže rozsah použití výjimky migrovat. Pokud je tak v rozsahu použití KSWS vybrána alespoň jedna součást, KES použije výjimku na všechny součásti aplikace.

Rozsah použití KSWS můžete nakonfigurovat v nastavení důvěryhodné zóny a rovněž v nastavení součásti ochrany KSWS. To provedete zaškrtnutím nebo zrušení zaškrtnutí políčka **Apply Trusted Zone** v odpovídající části zásad. Nastavení součástí ochrany KES toto políčko nezahrnuje. To znamená, že se stav důvěryhodné zóny u jednotlivých nastavení součásti při migraci ztratí. Po dokončení migrace v nastavení důvěryhodné zóny v zásadách KES vyberte součásti, na které se výjimka vztahuje.

Migrace poznámek

Poznámky z důvěryhodné zóny KSWS se migrují do poznámek u výjimek KES beze změn.

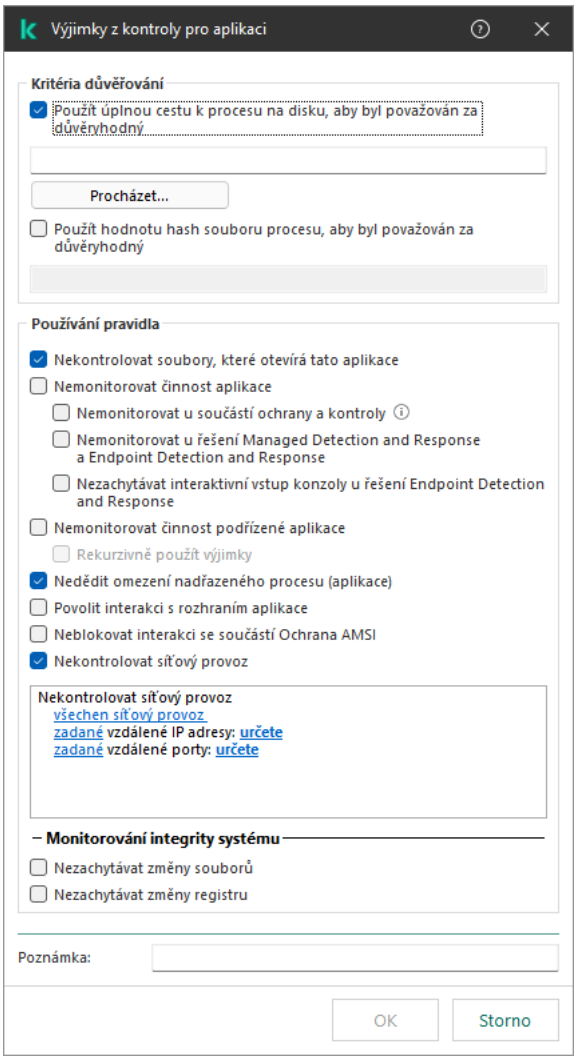
Migrace důvěryhodných procesů

Důvěryhodné proces KSWS se migrují do důvěryhodných procesů KES s několika omezeními. Migrace důvěryhodných procesů závisí na metodě výběru objektu:

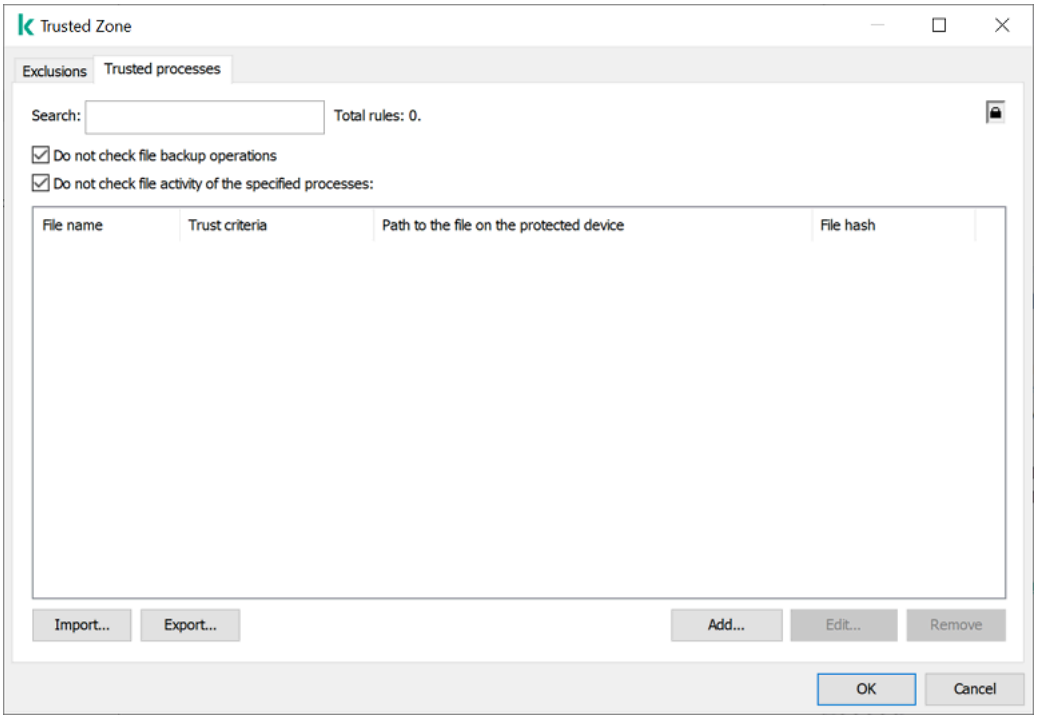
- Path to the file on the protected device – migruje se do důvěryhodných aplikací KES.
- File hash – *nemigruje se*.

Pokud má KSWS důvěryhodné procesy nakonfigurované jako hodnota hash souboru, tyto důvěryhodné procesy nebudou migrovány. Po migraci musíte tyto důvěryhodné procesy přidat ručně.

Je-li v nastavení důvěryhodného procesu zaškrtnuto políčko **Do not check file backup operations**, toto nastavení se migruje do důvěryhodných aplikací KES (políčko **Nemonitorovat činnost aplikace**).



Nastavení důvěryhodné aplikace KES



Nastavení důvěryhodného procesu KSWS

Migrace pravidel součásti KSWS Kontrola spouštění aplikací

Kontrola spouštění aplikací KSWS je standardně nastavena na blokování. To znamená, že součást Kontrola spouštění aplikací automaticky blokuje všechny aplikace, které nejsou uvedeny v pravidlech jako povolené aplikace. Proto průvodce migrací součásti KES Kontrola aplikací automaticky nastaví režim kontroly **Seznam povolených položek**, který odpovídá principu standardního blokování.

Pravidla můžete migrovat z KSWS do KES pomocí *průvodce hromadným převodem zásad a úloh* nebo *průvodce vytvořením nové zásady KES založené na zásadě KSWS*.

Migrace režimu součásti Kontrola spouštění aplikací

Režim součásti KSWS Kontrola spouštění aplikací lze migrovat do součásti KES Kontrola aplikací následujícím způsobem:

- **Statistics only** → **Otestovat pravidla**;
- **Active** → **Použít pravidla**.

Migrace předdefinovaných pravidel součásti KSWS Kontrola spouštění aplikací

Standardně Kontrola spouštění aplikací KSWS zahrnuje dvě pravidla:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

Předdefinovaná pravidla povolují spouštění *skriptů*, *balíčků MSI* a *spustitelných souborů* podepsaný důvěryhodným kořenovým certifikátem. Pokud je alespoň jedno předdefinované pravidlo KSWS typu **Allow**, průvodce migrací vytvoří nové povolující pravidlo, **Applications with trusted root certificates**. To znamená, že nástroj součást Kontrola aplikací KES používá pro povolení spouštění důvěryhodných skriptů, balíčků MSI a spustitelných souborů jedno pravidlo.

Pokud jsou obě předdefinovaná pravidla KSWS typu **Deny**, KES bude předdefinovaná pravidla ignorovat.

Migrace vlastních pravidel součásti KSWS Kontrola spouštění aplikací

Pravidla součásti KSWS Kontrola spouštění aplikací regulují spouštění souborů v souladu s následujícími kritérii:

- podpis digitálním certifikátem;
- SHA256 hash;
- cesta k souboru.

Pravidla se v KSWS a KES vytvářejí odlišně, proto vytvoří průvodce migrací *kategorie aplikací*, které zahrnují podmínky a výjimky z pravidel KSWS, a přidá tyto kategorie aplikací do pravidel KES. Průvodce použije v kategoriích aplikací **Certifikát**, **Cesta ke složce** a **Hodnota hash souboru**. Nové kategorie aplikací jsou k dispozici v konzole pro správu aplikace Kaspersky Security Center v části **Application management** → **Application categories**.

Průvodce migrací seskupí pravidla KSWS podle typu a podle uživatele. Dále průvodce vytvoří kategorie aplikací, které zahrnují podmínky a výjimky z pravidel KSWS, a přidá kategorie aplikací do nových pravidel KES. Průvodce zadá názvy pravidel KSWS do pole **Popis** pravidel KES.

Migrace rozšířeného nastavení součásti KSWS Kontrola spouštění aplikací

Princip fungování součásti KSWS Kontrola spouštění aplikací a součásti KES Kontrola aplikací se liší, takže průvodce migrací může migrovat podmnožinu nastavení.

Nastavení součásti Kontrola spouštění aplikací

Nastavení aplikace Kaspersky Security for Windows Server	Nastavení aplikace Kaspersky Endpoint Security pro systém Windows
Repeat action taken for the first file launch on all the subsequent launches for this file	*(nemigruje)* Kaspersky Endpoint Security kontroluje aplikaci pokaždé, když se pokusí spustit.
Deny the command interpreters launch with no command to execute	*(nemigruje)* Aplikace Kaspersky Endpoint Security umožňuje spouštění překladačů příkazů, pokud nejsou zakázány součástí Kontrola aplikací.
Apply rules to executable files	*(nemigruje)* Rozsah aplikace pravidla nelze nakonfigurovat v nastavení součásti Kontrola aplikací KES. Kontrola aplikací KES uplatňuje pravidla na všechny typy souborů: spustitelné soubory, skripty a balíčky MSI. Pokud jsou všechny typy souborů zahrnuty do rozsahu použití pravidel v KSWS, KES během migrace tato pravidla KSWS přenese. Pokud je některý typ souboru vyloučen z rozsahu použití pravidel v KSWS, KES během migrace přenese také pravidla KSWS, ale jako akce součásti Kontrola aplikací je vybrána možnost **Otestovat pravidla**.
Monitor loading of DLL modules	**Monitorovat zavádění modulů DLL (výrazně zvýší zatížení systému)**

Apply rules to scripts and MSI packages	*(nemigruje)* Rozsah aplikace pravidla nelze nakonfigurovat v nastavení součásti Kontrola aplikací KES. Kontrola aplikací KES uplatňuje pravidla na všechny typy souborů: spustitelné soubory, skripty a balíčky MSI. Pokud jsou všechny typy souborů zahrnuty do rozsahu použití pravidel v KSWS, KES během migrace tato pravidla KSWS přenese. Pokud je některý typ souboru vyloučen z rozsahu použití pravidel v KSWS, KES během migrace přenese pravidla KSWS, ale jako akce součásti Kontrola aplikací je vybrána možnost **Otestovat pravidla**.
Deny applications untrusted by KSN	*(nemigruje)* Kaspersky Endpoint Security nebere v úvahu reputaci aplikací a povoluje nebo zakazuje spouštění aplikací v souladu s pravidly.
Allow applications trusted by KSN	Během migrace KES přidá nové povolující pravidlo. Jako podmínka spuštění pravidla je zadána kategorie KL **Ostatní software\Aplikace, důvěryhodné podle reputace v KSN**.
Users and / or user groups allowed to run applications trusted by KSN	**Uživatelé a jejich práva** v povolujícím pravidle součásti Kontrola aplikací, které zahrnuje kategorii KL **Ostatní software\Aplikace, důvěryhodné podle reputace v KSN**.
Automatically allow software distribution via applications and packages listed	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru. Jako podmínka aktivace pravidla je zadán hash souboru.
Always allow software distribution via Windows Installer	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru (**Software distribution applications and packages allowed**). Jako podmínka aktivace pravidla je zadán hash souboru. Ve vlastnostech účtu je zaškrtnuto políčko **Důvěryhodné nástroje aktualizace**.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	*(nemigruje)*
Software distribution applications and packages allowed	Řízení distribuce softwaru v aplikacích KSWS a KES funguje odlišně. Během migrace přidá KES nová pravidla pro povolování aplikací, které mají povolenou automatickou distribuci softwaru. Jako podmínka aktivace pravidla je zadán hash souboru. Ve vlastnostech účtu je zaškrtnuto políčko **Důvěryhodné nástroje aktualizace**.
Schedule settings	*(nemigruje)* Pokud je pro součást v nastavení KSWS nakonfigurován plán, je součást Kontrola aplikací při migraci povolena. Jestliže pro součást v nastavení KSWS není nakonfigurován plán, je součást Kontrola aplikací při migraci zakázána. Pro součást není možné konfigurovat samostatný plán. Součást je vždy zapnutá, když je aplikace Kaspersky Endpoint Security v provozu.

Instalace KES místo KSWS

Aplikaci Kaspersky Endpoint Security můžete nainstalovat následujícími způsoby:

- Instalace KES po odebrání KSWS (doporučeno).
- Instalace KES na KSWS.

Odebrání aplikace Kaspersky Security for Windows Server

Aplikaci můžete odebrat vzdáleně pomocí úlohy *Uninstall application remotely*, případně lokálně na serveru. Po odebrání KSWS může být nutné restartovat server. Pokud chcete nainstalovat aplikaci Kaspersky Endpoint Security bez restartu, ujistěte se, že je aplikace Kaspersky Security for Windows Server zcela odebrána. Pokud aplikace není zcela odebrána, instalace aplikace Kaspersky Endpoint Security může způsobit chybnou činnost serveru. Ujištění, že je aplikace zcela odebrána, také doporučujeme, pokud jste použili nástroj kavremover. Nástroj kavremover nepodporuje správu KSWS.

Pokud je povolena ochrana heslem pro omezení přístupu ke KSWS, zadejte heslo pro odinstalaci v nastavení instalačního balíčku KES.

Po odstranění KSWS nainstalujte aplikaci Kaspersky Endpoint Security pro systém Windows jakýmkoli dostupným způsobem.

Instalace aplikace Kaspersky Endpoint Security

Když instalujete KES vzdáleně, na serveru jsou nainstalovány součásti, které jste vybrali ve vlastnostech instalačního balíčku. Doporučujeme vybrat výchozí součásti ve vlastnostech instalačního balíčku. Při instalaci KES nad KSWS není nutný restart.

Aplikace Kaspersky Endpoint Security před místní instalací zkontroluje přítomnost aplikací společnosti Kaspersky v počítači. Pokud je na počítači nainstalována aplikace Kaspersky Security for Windows Server, KES detekuje sadu součástí KSWS, které jsou nainstalovány, a vybere stejné součásti k instalaci. Při instalaci KES nad KSWS není nutný restart.

Pokud se instalace KES nad KSWS nezdařila, můžete ji vrátit zpět. Po vrácení instalace se doporučuje restartovat server a zkusit to znovu.

Nastavení a úlohy KSWS se nemigrují, když je nainstalována aplikace Kaspersky Endpoint Security pro systém Windows. Chcete-li migrovat nastavení a úlohy, spusťte průvodce hromadným převodem zásad a úloh.

Seznam nainstalovaných součástí si můžete prohlédnout v části **Zabezpečení** v rozhraní aplikace pomocí příkazu `status` nebo v konzole aplikace Kaspersky Security Center ve vlastnostech počítače. Sadu součástí můžete po instalaci změnit pomocí úlohy *Změna součástí aplikace*.

Migrace konfigurace [KSWS+KEA] na konfiguraci [KES+integrovaný agent]

Pro podporu používání aplikace Kaspersky Endpoint Security pro systém Windows v rámci řešení EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA a MDR byl do aplikace přidán integrovaný agent. Pro práci s těmito řešeními už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent.

Při migraci z KSWS na KES budou řešení EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA a MDR nadále spolupracovat s integrovanými agenty aplikace Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent.

Migrace konfigurace [KSWS+KEA] do konfigurace [KES+integrovaný agent] zahrnuje následující kroky:

1. **Migrace z KSWS na KES**

   Migrace z KSWS na KES zahrnuje instalaci aplikace Kaspersky Endpoint Security místo aplikace Kaspersky Security for Windows Server.

   Správci obvykle povolují ochranu heslem, aby omezili přístup k KSWS a KEA. Od verze aplikace Kaspersky Security Center Linux 15.1 můžete do nastavení úlohy *Install application remotely* přidávat heslo pro odinstalaci aplikace. Tato úloha umožňuje zadání pouze jednoho hesla pro odinstalaci. To znamená, že pokud je pro KSWS a KEA nastaveno stejné heslo, aplikace KSWS a KEA budou úspěšně odebrány. Pokud se hesla liší, odebrání jedné z aplikací se nezdaří s chybou přístupu. Chcete-li dokončit migraci, musíte vypnout ochranu heslem pro aplikaci, jejíž heslo jste nemohli zadat v nastavení úlohy *Install application remotely*.

   Chcete-li provést migraci, musíte vybrat součásti potřebné pro podporu řešení Detection and Response jako součást aplikace Kaspersky Endpoint Security. Po instalaci se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odebere aplikaci Kaspersky Endpoint Agent.

2. **Migrace zásady a úkolů**

   Migrace zásad a úloh [KSWS+KEA] do [KES+integrovaný agent] zahrnuje následující kroky:

   1. Migrace zásad a úloh z KSWS do KES pomocí Průvodce hromadným převodem zásad a úloh (k dispozici pouze v konzole pro správu (MMC)).

      Do zásady KES se tak přidá profil zásad s názvem *UpgradedFromKSWS <název zásady aplikace Kaspersky Security for Windows Server>*. Nové úlohy KES jsou také vytvářeny s názvy *<název úlohy KSWS> (converted)*.

   2. Migrace zásad a úloh z KEA na KES pomocí průvodce migrací z aplikace Kaspersky Endpoint Agent (k dispozici pouze ve webové konzole a cloudové konzole).

      Výsledkem je vytvoření nové zásady s názvem *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Vytvářejí se také nové úlohy a úlohy KES.

3. **Jak funguje licence**

   Pokud používáte k aktivaci aplikací Kaspersky Endpoint Security pro systém Windows a Kaspersky Endpoint Agent společnou licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security, funkce EDR Optimum bude aktivována automaticky po upgradu aplikace na verzi 11.7.0. Nemusíte dělat nic jiného.

   Jestliže používáte k aktivaci funkce EDR Optimum licenci k doplňku Kaspersky Endpoint Detection and Response Optimum, do úložiště aplikace Kaspersky Security Center se přidá klíč k doplňku EDR Optimum je povolena automatická distribuce licenčního klíče. Po upgradu aplikace na verzi 11.7.0 je funkce EDR Optimum aktivována automaticky.

   Pokud používáte k aktivaci aplikace Kaspersky Endpoint Agent licenci k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security a jinou licenci k aktivaci Kaspersky Endpoint Security pro systém Windows, musíte nahradit klíč k aplikaci Kaspersky Endpoint Security pro systém Windows společným klíčem k řešením Kaspersky Endpoint Detection and Response Optimum nebo Kaspersky Optimum Security. Klíč můžete nahradit pomocí úlohy *Add key*.

   Nemusíte aktivovat funkci Kaspersky Sandbox. Funkce Kaspersky Sandbox bude k dispozici okamžitě po upgradu a aktivaci aplikace Kaspersky Endpoint Security pro systém Windows.

K aktivaci aplikace Kaspersky Endpoint Security jako součásti řešení Kaspersky Anti Targeted Attack Platform lze použít pouze licenci k řešení Kaspersky Anti Targeted Attack Platform. Po upgradu aplikace na verzi 12.1 je funkce EDR (KATA) aktivována automaticky. Nemusíte dělat nic jiného.

4. **Kontrola stavu řešení Kaspersky Endpoint Detection and Response Optimum a Kaspersky Sandbox**

   Pokud je po upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

   - Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
   - Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*.
   - V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.

   Pomocí *Report on status of application components* zkontrolujte, zda je aktivována funkce EDR Optimum. Pokud je stav součásti *Není součástí licence*, zkontrolujte, zda je u EDR Optimum zapnuta funkce automatické distribuce licenčního klíče.

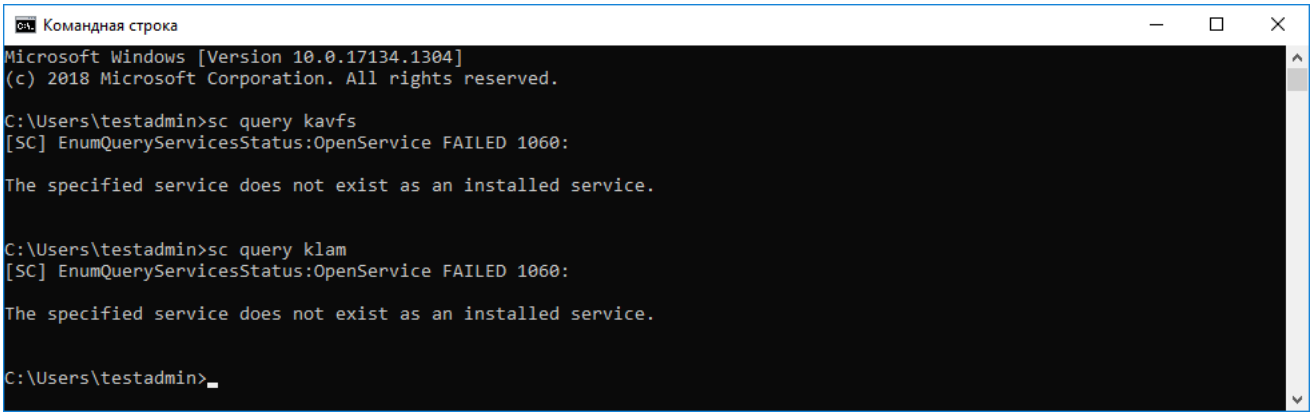
Ověření, že aplikace Kaspersky Security for Windows Server byla úspěšně odebrána

Ujistěte se, že je aplikace Kaspersky Security for Windows Server zcela odebrána:

- Neexistuje složka `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\`.
- Nejsou k dispozici následující služby:
  - Kaspersky Security Service (KAVFS)
  - Služba Kaspersky Security Management (KAVFSGT)
  - Služba Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Služba Kaspersky Security Script Checker (KAVFSSCS)

  Spuštěné služby můžete zkontrolovat ve Správci úloh nebo zadáním příkazu `sc query` (viz obrázek níže).
- Nejsou přítomny následující ovladače:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

  Nainstalované ovladače můžete zkontrolovat ve složce `C:\Windows\System32\drivers` složky nebo zadáním příkazu `sc query`. Pokud služba nebo ovladač chybí, obdržíte následující odpověď:



Ověření, zda byly služby a ovladače aplikace Kaspersky Security for Windows Server úspěšně odebrány

Pokud na serveru zůstanou soubory aplikace nebo ovladače, odstraňte příslušné soubory ručně. Pokud na serveru stále běží služby aplikace Kaspersky Security for Windows Server, zastavte (`sc stop`) a odstraňte (`sc delete`) tyto služby ručně. Chcete-li zastavit ovladač klam.sys, použijte příkaz `fltmc unload klam`.

Aktivace KES pomocí klíče KSWS

Po instalaci aplikace můžete aktivovat Kaspersky Endpoint Security pro systém Windows (KES) pomocí licenčního klíče aplikace Kaspersky Security for Windows Server (KSWS). Proces aktivace po migraci závisí na způsobu aktivace KSWS (viz tabulka níže).

Kaspersky Endpoint Security nepodporuje *licenci ke Kaspersky Security for Storage*. Chcete-li pracovat s touto licencí, musíte používat aplikaci Kaspersky Security for Windows Server.

Pro aktivaci aplikace KES pomocí klíče pro KSWS můžete použít pouze aktivační kód. Pokud k aktivaci aplikace používáte soubor klíče, musíte kontaktovat technickou podporu a získat od ní soubor klíče aplikace Kaspersky Endpoint Security.

Aktivace aplikace Kaspersky Endpoint Security pro systém Windows pomocí klíče Kaspersky Security for Windows Server

Způsob aktivace aplikace Kaspersky Security for Windows Server	Migrace klíče aplikace Kaspersky Endpoint Security pro systém Windows.
Automatická distribuce licenčního klíče KSWS do počítačů.	Pokud je ve vlastnostech licenčního klíče KSWS povolena automatická distribuce klíčů, KES se automaticky aktivuje pomocí klíče KSWS.
Klíč KSWS je přidán úlohou.	Pokud je vaše aplikace KSWS aktivována pomocí úlohy, licenční klíč KSWS se během migrace z KSWS odstraní. Aplikaci musíte znovu aktivovat. Můžete například přidat licenční klíč do instalačního balíčku Kaspersky Endpoint Security pro systém Windows.
Klíč KSWS se přidává lokálně v rozhraní aplikace.	Pokud je vaše aplikace KSWS aktivována lokálně pomocí průvodce aktivací aplikace, licenční klíč KSWS se během migrace z KSWS odstraní. Aplikaci musíte znovu aktivovat. Můžete například přidat licenční klíč do instalačního balíčku Kaspersky Endpoint Security pro systém Windows.
Klíč KSWS je přidán do instalačního balíčku.	Pokud je vaše KSWS aktivováno pomocí klíče z instalačního balíčku, licenční klíč KSWS se při migraci z KSWS odstraní. Aplikaci musíte znovu aktivovat. Můžete například přidat licenční klíč do instalačního balíčku Kaspersky Endpoint Security pro systém Windows.
Placená image virtuálního počítače (Amazon Machine Image – AMI) v Amazon Web Services (AWS).	Pokud jste zakoupili Kaspersky Security Center jako placenou image virtuálního stroje (Amazon Machine Image – AMI) v Amazon Web Services (AWS), aktivace KES není nutná. V tomto případě Kaspersky Security Center používá předplatné AWS, které je již přidáno do aplikace.
Hotová bezplatná image Kaspersky Security Center s vaší vlastní licencí (model BYOL – Bring Your Own License).	Pokud používáte předinstalovanou bezplatnou image aplikace Kaspersky Security Center s vlastní licencí v cloudovém prostředí (model BYOL – Bring Your Own License), musíte aplikaci aktivovat jakýmkoli dostupným způsobem. Budete potřebovat licenci pro Kaspersky Hybrid Cloud Security.

Zvláštní aspekty migrace serverů s vysokou zátěží

Na serverech s vysokou zátěží je důležité sledovat výkon a předcházet chybám. Po migraci na aplikaci Kaspersky Endpoint Security pro systém Windows doporučujeme dočasně zakázat součásti aplikace, které ve srovnání s ostatními součástmi využívají značné prostředky serveru. Poté, co se ujistíte, že server funguje normálně, můžete součásti aplikace znovu povolit.

Migraci serverů s vysokou zátěží doporučujeme provádět takto:

1. Vytvořte zásadu aplikace Kaspersky Endpoint Security s výchozím nastavením.

   Výchozí nastavení jsou považována za optimální. Tato nastavení doporučují odborníci společnosti Kaspersky. Výchozí nastavení poskytují doporučenou úroveň ochrany a optimální využití zdrojů.

2. V nastavení zásady vypněte následující součásti: Ochrana před síťovými hrozbami, Detekce chování, Prevence zneužití, Modul pro nápravu, Kontrola aplikací.

   Pokud má vaše organizace nasazeno řešení Kaspersky Managed Detection and Response (MDR), nahrajte konfigurační soubor BLOB do zásad aplikace Kaspersky Endpoint Security.

3. Odeberte aplikaci Kaspersky Security for Windows Server ze serveru.

4. Nainstalujte aplikaci Kaspersky Endpoint Security pro systém Windows s výchozí sadou součástí.

   Pokud má vaše organizace nasazena řešení Detection and Response, vyberte ve vlastnostech instalačního balíčku příslušné součásti.

5. Zkontrolujte nastavení aplikace:

   - Aplikace se aktivuje licenčním klíčem KSWS.
   - Použijí se nové zásady. Dříve vybrané součásti jsou zakázány.

6. Ujistěte se, že server funguje. Ujistěte se, že aplikace Kaspersky Endpoint Security pro systém Windows nevyužívá více než 1 % zdrojů serveru.

7. V případě potřeby vytvořte výjimky z kontroly, přidejte důvěryhodné aplikace a vytvořte seznam důvěryhodných webových adres.

8. Zapněte součásti Detekce chování, Prevence zneužití a Modul pro nápravu. Ujistěte se, že aplikace Kaspersky Endpoint Security pro systém Windows nevyužívá více než 1 % zdrojů serveru.

9. Zapněte součást Ochrana před síťovými hrozbami. Ujistěte se, že aplikace Kaspersky Endpoint Security pro systém Windows nevyužívá více než 2 % zdrojů serveru.

10. Zapněte součást Kontrola aplikací v režim testování pravidel.

11. Ujistěte se, že funguje součást Kontrola aplikací. V případě potřeby po potvrzení funkčnosti součásti Kontrola aplikací přidejte nová pravidla této součásti a vypněte režim testování pravidel.

Po migraci z KSWS na KES se ujistěte, že aplikace funguje správně. V konzole kontrolujte stav serveru (měl by být *OK*). Ujistěte se, že pro aplikaci nejsou hlášeny žádné chyby, zkontrolujte také čas posledního připojení k serveru pro správu, čas poslední aktualizace databáze a stav ochrany serveru.

Správa aplikace na serveru v režimu Server Core

Server v režimu Server Core nemá grafické uživatelské rozhraní (GUI). Proto můžete aplikaci spravovat pouze vzdáleně pomocí konzoly aplikace Kaspersky Security Center nebo místně z příkazového řádku.

Správa aplikace pomocí konzoly aplikace Kaspersky Security Center

Instalace aplikace pomocí konzoly aplikace Kaspersky Security Center se neliší od instalace běžným způsobem. Když vytváříte instalační balíček, můžete přidat licenční klíč pro aktivaci aplikace. Můžete použít klíč aplikace Kaspersky Endpoint Security pro systém Windows nebo klíč aplikace Kaspersky Security for Windows Server.

> Na serveru v režimu Server Core nejsou k dispozici následující součásti aplikace: Ochrana před webovými hrozbami, Ochrana před hrozbami v poště, Kontrola webu, Ochrana před útoky BadUSB, Šifrování na úrovni souborů (FLE), Kaspersky Disk Encryption (FDE).

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. Aplikace nemůže zobrazit okno s výzvou k restartování serveru. O nutnosti restartovat server se můžete dozvědět ze zpráv v konzole aplikace Kaspersky Security Center.

Správa aplikace na serveru v režimu Server Core se neliší od správy počítače. Ke konfiguraci aplikace můžete použít zásady a úlohy.

Při správě aplikace na serverech v režimu Server Core je nutno brát v úvahu tyto zvláštní aspekty:

- Server v režimu Server Core nemá grafické uživatelské rozhraní, proto aplikace Kaspersky Endpoint Security nezobrazuje varování informující uživatele o nutnosti pokročilé dezinfekce. Chcete-li dezinfikovat hrozbu, musíte v nastavení aplikace povolit technologii pokročilé dezinfekce a v nastavení úlohy *Kontrola malwaru* povolit okamžitou pokročilou dezinfekci. Poté musíte spustit úlohu *Kontrola malwaru*.

- Technologie BitLocker Drive Encryption je k dispozici pouze s modulem TPM (Trusted Platform Module). PIN/heslo nelze použít pro šifrování, protože aplikace není schopna zobrazit okno s výzvou k zadání hesla pro ověření před spuštěním. Pokud má operační systém povolený režim kompatibility FIPS (Federal Information Processing Standard), připojte vyměnitelnou jednotku pro uložení šifrovacího klíče, než začnete jednotku šifrovat.

Správa aplikace z příkazového řádku

Když nemůžete použít grafické rozhraní aplikace, můžete spravovat aplikaci Kaspersky Endpoint Security z příkazového řádku.

Chcete-li nainstalovat aplikaci na server v režimu Server Core, zadejte následující příkaz:

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s

Chcete-li aplikaci aktivovat, zadejte následující příkaz:

avp.com license /add <activation code or key file>

Chcete-li zkontrolovat stavy profilu aplikace, zadejte následující příkaz:

avp.com status

Chcete-li zobrazit seznam příkazů správy aplikací, zadejte následující příkaz:

avp.com help

Migrace z [KSWS+KEA] na [KES+integrovaný agent]

Při migraci z aplikace Kaspersky Security for Windows Server (KSWS) na aplikaci Kaspersky Endpoint Security (KES) můžete ke konfiguraci ochrany serveru a optimalizaci výkonu použít následující doporučení. Zde se podíváme na příklad migrace pro jednu organizaci.

Infrastruktura organizace

Společnost má instalováno následující vybavení:

- Kaspersky Security Center 14.2

  Správce spravuje řešení Kaspersky pomocí konzoly pro správu (MMC). Je rovněž nasazeno řešení Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)

  V aplikaci Kaspersky Security Center jsou vytvořeny tři skupiny správy obsahující servery organizace: dvě skupiny správy pro servery SQL a skupina správy pro servery Microsoft Exchange. Každá skupina správy je řízena vlastní zásadou. Jsou vytvořeny úlohy *Database Update* a *On-demand scan* pro všechny servery v organizaci.

  Aktivační klíč KSWS je přidán do aplikace Kaspersky Security Center. Je povolena automatická distribuce klíčů.

- Servery SQL s nainstalovanou aplikací Kaspersky Security for Windows Server 11.0.1 a Kaspersky Endpoint Agent 3.11. Servery SQL jsou sloučeny do dvou clusterů.

  Aplikaci KSWS spravují zásady *SQL_Policy(1)* a *SQL_Policy(2)*. Jsou také vytvořeny úlohy *Database Update* a *On-demand scan*.

- Server Microsoft Exchange s nainstalovanou aplikací Kaspersky Security for Windows Server 11.0.1 a Kaspersky Endpoint Agent 3.11.

  Aplikaci KSWS spravuje zásada *Exchange_Policy*. Jsou také vytvořeny úlohy *Database Update* a *On-demand scan*.

Plánování migrace

Migrace zahrnuje následující kroky:

1. Migrace úloh a zásad KSWS pomocí průvodce hromadným převodem zásad a úloh.
2. Migrace zásad aplikace Kaspersky Endpoint Agent pomocí průvodce hromadným převodem zásad a úloh.
3. Použití značek k aktivaci profilů zásad ve vlastnostech nové zásady.
4. Instalace KES místo KSWS.
5. Aktivace řešení EDR Optimum.
6. Potvrzení, že KES funguje.

Scénář migrace se zpočátku provádí na jednom z clusteru serverů SQL. Poté se scénář migrace provede na jiném clusteru serverů SQL. Poté se scénář migrace provede na serveru Microsoft Exchange.

Migrace úloh a zásad KSWS pomocí průvodce hromadným převodem zásad a úloh

Chcete-li migrovat úlohy KSWS, můžete použít průvodce hromadným převodem zásad a úloh (průvodce migrací). Výsledkem je, že místo zásad *SQL_Policy(1)*, *SQL_Policy(2)* a *Exchange_Policy* získáte jednu zásadu se třemi profily pro servery SQL a Microsoft Exchange. Nový profil zásad s nastavením KSWS bude pojmenován *UpgradedFromKSWS<název zásady aplikace Kaspersky Security for Windows Server>*. Ve vlastnostech profilu průvodce migrací automaticky vybere jako aktivační kritérium značku `UpgradedFromKSWS`. Nastavení z profilu zásad se tedy na servery aplikují automaticky.

Migrace zásad aplikace Kaspersky Endpoint Agent pomocí průvodce hromadným převodem zásad a úloh

Chcete-li migrovat zásady aplikace Kaspersky Endpoint Agent, můžete použít průvodce hromadným převodem zásad a úloh. Průvodce migrací zásad a úloh pro aplikaci Kaspersky Endpoint Agent je k dispozici pouze ve webové konzole.

Použití značek k aktivaci profilů zásad ve vlastnostech nové zásady

Vyberte značku zařízení, kterou jste dříve přiřadili jako podmínku aktivace profilu. Otevřete vlastnosti zásad a jako podmínku aktivace profilu vyberte *General rules for policy profile activation*.

Instalace KES místo KSWS

Před instalací aplikace KES musíte zakázat ochranu heslem ve vlastnostech zásad aplikace KSWS.

Instalace aplikace KES zahrnuje následující kroky:

1. Připravte si instalační balíček. Ve vlastnostech instalačního balíčku vyberte distribuční sadu Kaspersky Endpoint Security pro systém Windows 12.0 a vyberte výchozí sadu součástí.
2. Vytvořte úlohu *Install application remotely* pro jednu ze skupin správy serveru SQL.
3. Ve vlastnostech úlohy vyberte instalační balíček a soubor licenčního klíče.

4. Počkejte, až bude úloha úspěšně dokončena.

5. Opakujte instalaci aplikace KES pro zbývající skupiny správy.

Po dokončení instalace aplikace KES přidá aplikace Kaspersky Security Center automaticky k názvům počítačů v konzole značku `UpgradedFromKSWS`.

Chcete-li zkontrolovat instalaci aplikace KES, můžete použít úlohu *Report on protection deployment*. Můžete také zkontrolovat stav zařízení. Pro potvrzení aktivace aplikace můžete použít úlohu *Report on usage of license keys*.

Aktivace EDR Optimum

Funkci EDR Optimum můžete aktivovat pomocí samostatné licence k doplňku Kaspersky Endpoint Detection and Response Optimum. Musíte potvrdit, že je klíč k EDR Optimum přidán do úložiště aplikace Kaspersky Security Center a je povolena funkce automatické distribuce licenčního klíče.

Chcete-li zkontrolovat aktivaci EDR Optimum, můžete použít úlohu *Report on status of application components*.

Potvrzení, že KES funguje

Chcete-li potvrdit, že KES funguje, můžete zkontrolovat, zda nejsou hlášeny žádné chyby. Stav zařízení musí být *OK*. Úlohy aktualizace a kontroly malwaru byly úspěšně dokončeny.

Režim Light Agent pro ochranu virtuálních počítačů



Počínaje verzí 12.8 můžete používat aplikaci Kaspersky Endpoint Security pro systém Windows jako součást řešení Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* je integrované řešení, které poskytuje komplexní ochranu virtuálních strojů před různými typy hrozeb v oblasti informační bezpečnosti, síťovými útoky a phishingovými útoky. Chcete-li používat toto řešení, musíte aplikaci nainstalovat v režimu Light Agent.

Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent na virtuálních počítačích s architekturou ARM není podporována.

Aplikaci Kaspersky Endpoint Security můžete používat v režimu Light Agent jako součást řešení Kaspersky Security for Virtualization Light Agent počínaje verzí 6.2.

Když spustíte součást Light Agent, naváže a udrží připojení k virtuálnímu počítači SVM (Secure Virtual Machine). Na SVM je nasazen server pro ochranu. *Server pro ochranu* je součást řešení Kaspersky Security for Virtualization Light Agent, která kontroluje soubory na výskyt virů a jiného malwaru, aktualizuje antivirové databáze a spravuje licenční klíče. Light Agent odesílá fragmenty souborů, které vyžadují kontrolu, na SVM. Výsledky kontroly jsou k dispozici pro všechny virtuální počítače s nainstalovanou součástí Light Agent (technologie SharedCache). SharedCache tak zvyšuje efektivitu řešení a poskytuje rychlejší reakci na hrozby.

Infrastruktura organizace může obsahovat více virtuálních počítačů s nainstalovanou součástí Light Agent a více serverů SVM. Součást Integrační server je určena pro interakci mezi součástmi řešení a virtuální infrastrukturou. *Integrační server* – součást řešení Kaspersky Security for Virtualization Light Agent, která generuje seznam dostupných serverů SVM a přenáší tato data do součástí Light Agent, podílí se na zjišťování serverů SVM pomocí součástí Light Agent, zabezpečuje připojení mezi součástmi Light Agent a SVM a plní další funkce.

Zvláštní opatření pro režim Light Agent

Aplikaci Kaspersky Endpoint Security můžete spravovat ve standardním režimu a režimu Light Agent pomocí zásad a úloh aplikace Kaspersky Endpoint Security. V režimu Light Agent nejsou k dispozici některé součásti a funkce aplikace.

Aktualizace databází a softwarových modulů aplikace

Aplikace Kaspersky Endpoint Security v režimu Light Agent používá zvláštní databáze malwaru, které potřebuje, když funguje v rámci řešení Kaspersky Security for Virtualization Light Agent. Aplikace Kaspersky Endpoint Security získává aktualizace databází a modulů aplikací ze serveru pro ochranu.

Databáze a moduly na chráněných virtuálních počítačích jsou aktualizovány pomocí zvláštní úlohy *Aktualizace databází a modulů aplikace*, ve které je jako aktualizační zdroj zadána složka na SVM. Light Agent spouští úlohu *Aktualizace databází a modulů aplikace* automaticky. Nelze vybrat jiný zdroj aktualizací, konfigurovat plán úlohy ani úlohu odebrat.

Vrácení nejnovější aktualizace databáze malwaru je také řešeno na straně serveru pro ochranu. Po vrácení aktualizace databází a modulů aplikace v SVM se na chráněném virtuálním počítači spustí zvláštní místní úloha *Aktualizace databází a modulů aplikace*. Tato úloha přiměje součást Light Agent vrátit se k používání předchozí sady databází malwaru.

Aplikace Kaspersky Endpoint Security v režimu Light Agent nepodporuje úlohu *Vrácení aktualizace zpět*.

Aktivace součásti Light Agent

Chcete-li aktivovat aplikaci, musíte na server SVM, ke které je součást Light Agent připojena, přidat licenční klíč. Aplikaci není potřeba samostatně aktivovat.

Další zvláštní aspekty u režimu Light Agent

- Při vytváření zásad pro aplikaci doporučujeme vybrat režim Light Agent. V tomto režimu vás průvodce novou zásadou vyzve ke konfiguraci připojení SVM. Toto nastavení je nutné, aby aplikace fungovala v režimu Light Agent.
- V režimu Light Agent nelze instalovat součásti Šifrování dat ani Adaptivní kontrola anomálií. Kombinace součástí také závisí na typu hostovaného operačního systému: pracovní stanice nebo server.
- Light Agent nepodporuje integraci s řešením Kaspersky Endpoint Detection and Response Expert (cloud).
- Součást Light Agent můžete spravovat v konzole pro správu (MMC) a webové konzole aplikace Kaspersky Security Center. V cloudové konzole aplikace Kaspersky Security Center nelze součást Light Agent spravovat.
- Změna kombinace součástí aplikace na virtuálních počítačích VDI není podporována.
- Kaspersky Endpoint Security komunikuje se servery KSN prostřednictvím proxy serveru KSN. Přímá komunikace s KSN není podporována.
- Cloudový režim služby Kaspersky Security Network není podporován.
- Použití proxy serveru aplikace při připojování k integračnímu serveru (VIIS), serveru pro ochranu (SVM) a serverům KSN není podporováno.

Předběžná konfigurace virtuálního počítače

Kaspersky Endpoint Security můžete nainstalovat na virtuální počítač, který používá technologii virtuální platformy. Kaspersky Endpoint Security podporuje virtuální platformy VMware, Microsoft Hyper-V, Citrix. Před instalací musíte provést předběžnou konfiguraci virtuálních počítačů.

Kompatibilita s technologií Citrix App Layering

Pokud máte v úmyslu použít Full User Layer pro uložení stavu dočasných virtuálních počítačů, musíte před instalací virtuálních počítačů do šablony provést následující:

1. Vytvořte soubor C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt a přidat do něj následující výjimky:
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. V registru operačního systému v klíči HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr vytvořte novou hodnotu DWORD s názvem MiniFilterBypass a nastavte ji na 1.
3. V registru operačního systému v klíči HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd vytvořte novou hodnotu MULTI_SZ s názvem ExcludeKey a nastavte ji na \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.
4. Restartujte virtuální počítač.

Pro instalaci na virtuální stroje v infrastruktuře, která používá Citrix App Layering, musíte provést následující:

1. Nainstalujte agenta pro správu aplikace Kaspersky Security Center a Kaspersky Endpoint Security pro systém Windows do šablony virtuálního počítače v aplikační vrstvě.
2. Vytvořte virtuální kopii virtuálního stroje skládající se z více vrstev.
3. Nasaďte vytvořenou bitovou kopii na hypervizory, které podporují řešení Citrix App Layering.
4. Nakonfigurujte vytváření dočasných virtuálních počítačů z vytvořeného bitové kopie.

Podrobnosti o instalaci antivirového softwaru spolu s aplikací Citrix App Layering naleznete v dokumentaci k aplikaci Citrix App Layering.

Kompatibilita s technologií Citrix Provisioning (Citrix Provisioning Services)

Postup ujištění, že je aplikace kompatibilní s technologií Citrix Provisioning (Citrix Provisioning Services):

- Pokud je na virtuálním počítači nainstalován software Citrix Provisioning Target Device, musíte jej před instalací aplikace Kaspersky Endpoint Security odebrat. Po instalaci aplikace musíte nainstalovat Citrix Provisioning Target Device.

- Při instalaci aplikace pomocí průvodce nastavením nebo vzdáleně pomocí Kaspersky Security Center musíte zaškrtnout políčko **Zajistit kompatibilitu s Citrix PVS**.

Kompatibilita s technologií Omnissa App Volumes

Před instalací do šablony virtuálních počítačů musíte vytvořit soubor %SVAgent%\Config\Custom\snapvol.cfg a přidat do něj následující výjimky:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

Podrobnosti o rozhraní AMSI najdete v dokumentaci k aplikaci Omnissa.

Instalace součásti Light Agent

Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent na virtuálních počítačích s architekturou ARM není podporována.

Instalace aplikace v režimu Light Agent je stejná jako ve standardním režimu. Před instalací součásti Light Agent na virtuální počítač se musíte ujistit, že je nainstalována aplikace Kaspersky Security Center Network Agent. *Network Agent* usnadňuje interakci mezi serverem pro správu a virtuálním počítačem.

Součást Light Agent lze do virtuálního počítače nainstalovat jedním z následujících způsobů:

- Vzdáleně prostřednictvím aplikace Kaspersky Security Center.
- Místně pomocí průvodce instalací.
- Místně z příkazového řádku.

Chcete-li nainstalovat Light Agent, musíte vybrat vhodnou konfiguraci v nastavení instalačního balíčku nebo v průvodci instalací.

Při instalaci součásti Light Agent na server jsou součásti rozšířené ochrany (Detekce chování, Prevence zneužití, Modul pro nápravu) vyloučeny z výchozí konfigurace aplikace. Výchozí nastavení aplikace poskytuje doporučenou úroveň ochrany a optimální využití prostředků serveru. Při instalaci součásti Light Agent na pracovní stanici jsou součásti rozšířené ochrany zahrnuty ve výchozí konfiguraci aplikace.

Při instalaci součásti Light Agent doporučujeme vybrat předdefinované výjimky a důvěryhodné aplikace pro příslušné virtuální prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám pomohou rychle nastavit aplikaci a vyhnout se problémům s kompatibilitou virtuálního prostředí. Po instalaci můžete v zásadách také nakonfigurovat předdefinované výjimky z kontroly a důvěryhodné aplikace.

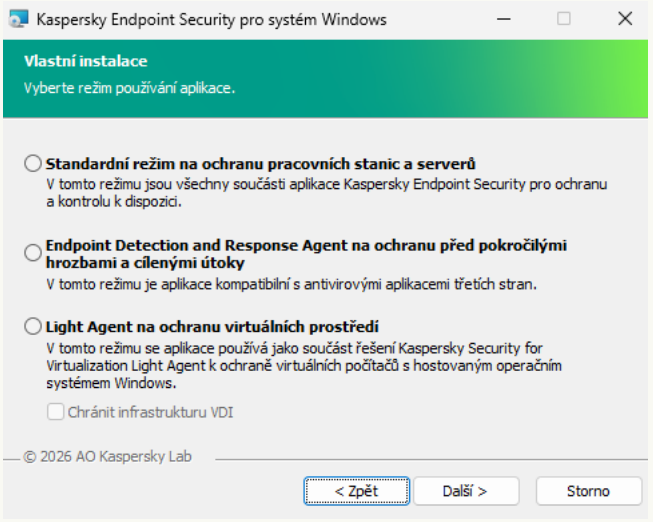
Při instalaci součásti Light Agent na trvalé virtuální počítače bude pravděpodobně potřeba změnit algoritmus generování Sensor ID. Sensor ID se v řešení Kaspersky Anti Targeted Attack Platform používá k identifikaci počítačů, které odesílají telemetrii na server. Chcete-li vytvořit jedinečné Sensor ID, nastavte při instalaci aplikace z příkazového řádku hodnotu `EnableUniqueSensorID=1`.

Jak nainstalovat Light Agent pomocí průvodce instalaci

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

Spustí se Průvodce instalací.

Konfigurace aplikace Kaspersky Endpoint Security



Výběr konfigurace aplikace

Vyberte konfiguraci **Light Agent na ochranu virtuálních prostředí**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Chránit infrastrukturu VDI** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

Součásti aplikace Kaspersky Endpoint Security

Vyberte součásti, které chcete nainstalovat (viz obrázek níže). Dostupné součásti aplikace můžete změnit po instalaci aplikace. Chcete-li tak učinit, musíte znovu spustit průvodce instalací a zvolit změnu dostupných součástí.

Rozšířené nastavení



Rozšířené nastavení instalace aplikace

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 Windows Remote Desktop), doporučujeme ochranu instalace vypnout.

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

Přidejte cestu k souboru avp.com do systémové proměnné %PATH%. Můžete přidat cestu instalace k proměnné %PATH% pro praktické použití rozhraní příkazového řádku.

Jak nainstalovat součást Light Agent pomocí 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:

   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]

   nebo

   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]

   Možnost `VDI` povoluje režim ochrany VDI (Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů. Režim ochrany VDI je ve výchozím nastavení povolen.

Součást Light Agent se tak na virtuální počítač instaluje s výchozí kombinací součástí. Kombinaci součástí můžete upravit a rozšířené nastavení zadat pomocí souboru setup.ini. Můžete také určit nastavení instalace na příkazovém řádku.

Jak nainstalovat Light Agent pomocí konzoly pro správu (MMC)

1. Otevřete konzolu pro správu aplikace Kaspersky Security Center.
2. Ve stromu konzole vyberte možnosti **Advanced** → **Remote installation** → složku **Installation packages**.

   Otevře se seznam instalačních balíčků, které byly staženy do aplikace Kaspersky Security Center.
3. Otevřete vlastnosti instalačního balíčku aplikace Kaspersky Endpoint Security pro systém Windows.

   Pokud je potřeba, vytvořte nový instalační balíček.
4. Přejděte do části **Settings**.
5. Vyberte konfiguraci **Light Agent na ochranu virtuálních prostředí**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuální počítače*, zaškrtněte políčko **Chránit infrastrukturu VDI**

(VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

6. Vyberte součásti, který chcete nainstalovat.

   Dostupné součásti aplikace můžete změnit po instalaci aplikace.

7. Nakonfigurujte důvěryhodnou zónu. Vyberte předdefinované výjimky z kontroly a důvěryhodné aplikace pro virtuální prostředí, do kterého aplikaci instalujete.

   Předdefinované výjimky z kontroly a důvěryhodné aplikace vám pomohou rychle nastavit aplikaci a vyhnout se problémům s kompatibilitou virtuálního prostředí.

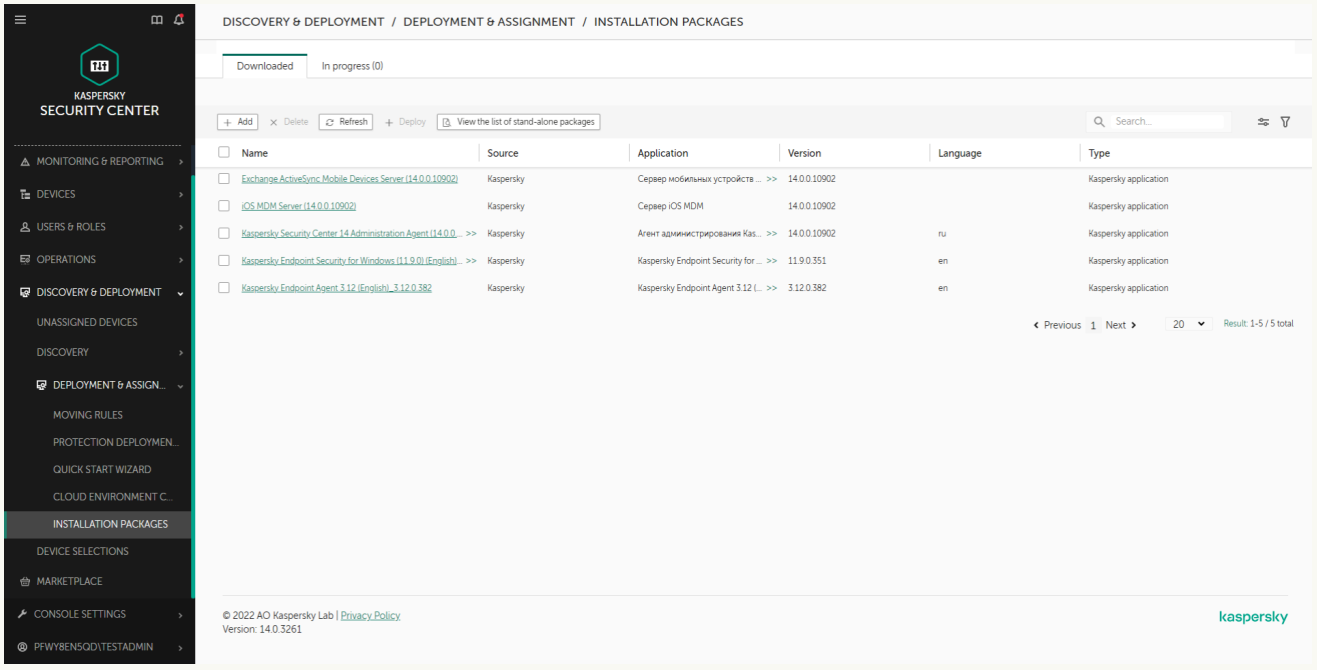
8. Uložte změny.

9. Vytvořte úlohu vzdálené instalace. Ve vlastnostech úlohy vyberte instalační balíček, který jste vytvořili.

Jak nainstalovat Light Agent pomocí webové konzoly

1. V hlavním okně webové konzoly vyberte možnosti **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

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



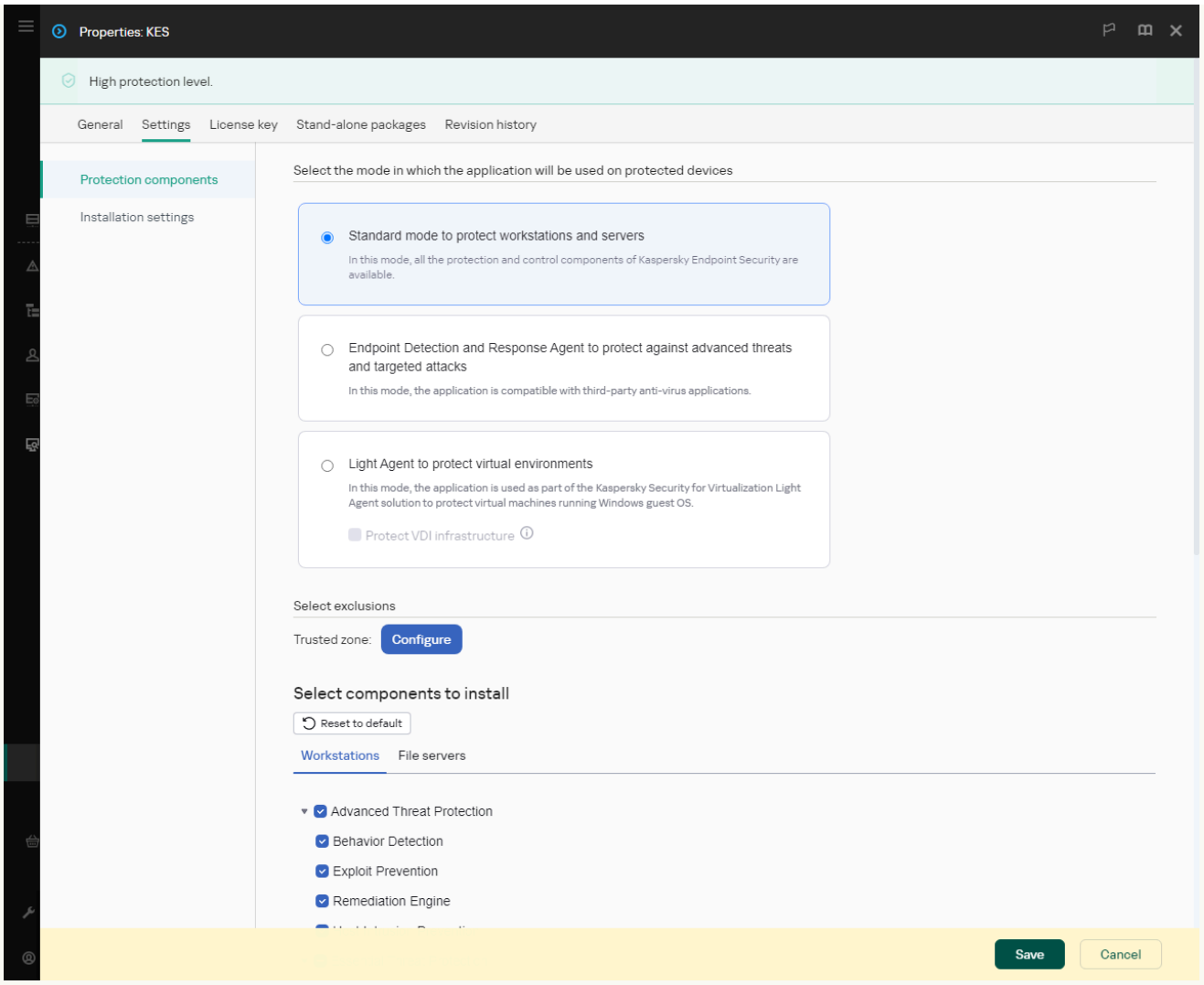
Seznam instalačních balíčků

2. Otevřete vlastnosti instalačního balíčku aplikace Kaspersky Endpoint Security pro systém Windows.

   Pokud je potřeba, vytvořte nový instalační balíček.

3. Vyberte kartu **Settings**.

4. Přejděte do části **Protection components**.



Součásti obsažené v instalačním balíčku

5. Vyberte konfiguraci **Light Agent to protect virtual environments**. Tato konfigurace je určena pro aplikaci, která se používá jako součást řešení Kaspersky Security for Virtualization Light Agent. Součást Light Agent musí být nainstalována na každý virtuální počítač, který je třeba pomocí řešení chránit. V této konfiguraci nelze použít součásti Šifrování dat ani součást Adaptivní kontrola anomálií. Pokud instalujete Light Agent na šablonu virtuálního počítače, která bude použita k vytvoření *neperzistentního virtuálního počítače*, zaškrtněte políčko **Protect VDI infrastructure** (VDI znamená Virtual Desktop Infrastructure). Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. V tomto režimu odmítne Light Agent aktualizace aplikací, které vyžadují restartování virtuálního počítače. Při příjmu aktualizací aplikace, které vyžadují restartování, Light Agent vygeneruje událost o potřebě aktualizovat šablonu chráněných virtuálních počítačů.

6. Vyberte součásti, který chcete nainstalovat.

   Dostupné součásti aplikace můžete změnit po instalaci aplikace.

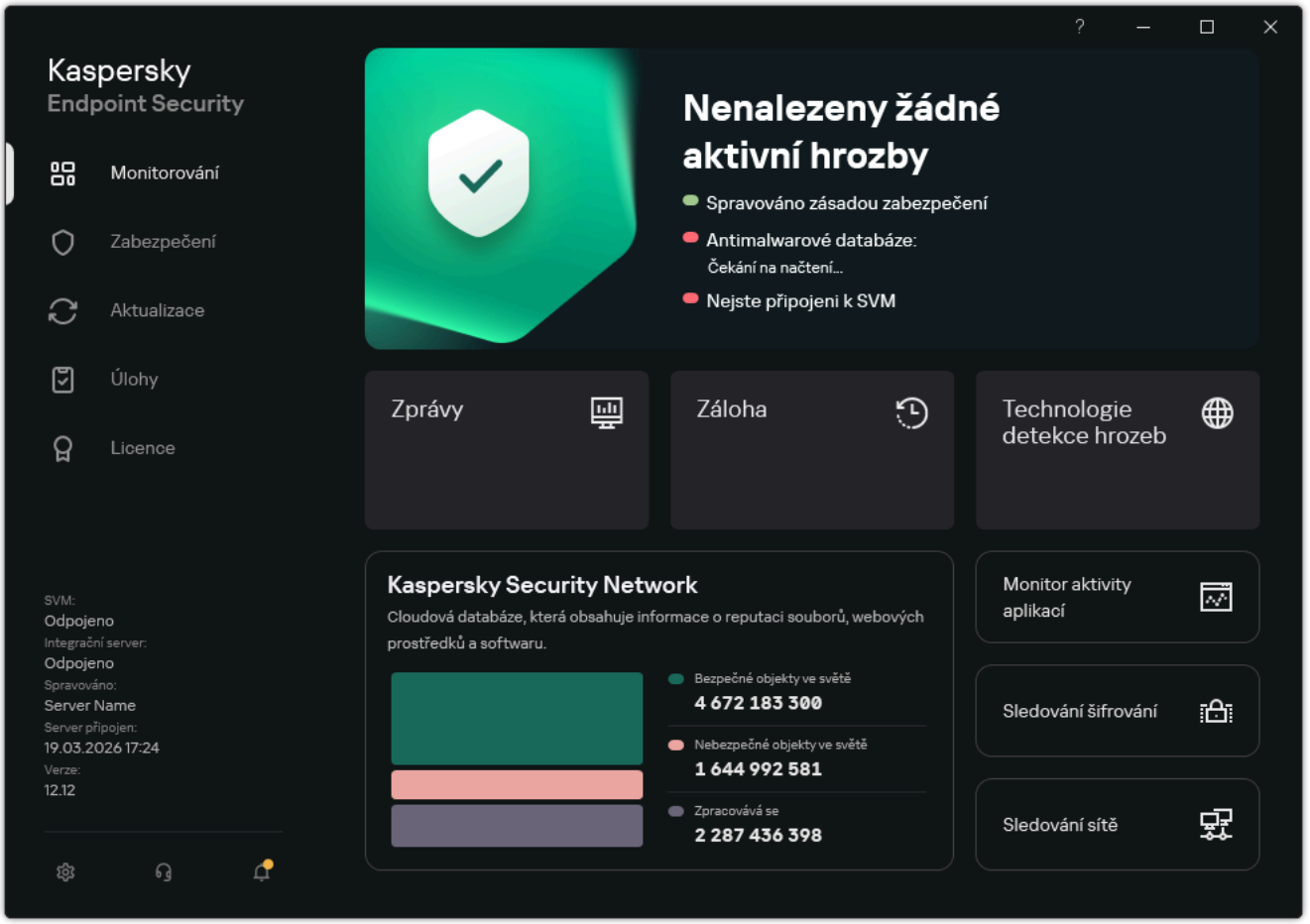
7. Nakonfigurujte důvěryhodnou zónu. Vyberte předdefinované výjimky z kontroly a důvěryhodné aplikace pro virtuální prostředí, do kterého aplikaci instalujete.

   Předdefinované výjimky z kontroly a důvěryhodné aplikace vám pomohou rychle nastavit aplikaci a vyhnout se problémům s kompatibilitou virtuálního prostředí.

8. Uložte změny.

9. Vytvořte úlohu vzdálené instalace. Ve vlastnostech úlohy vyberte instalační balíček, který jste vytvořili.

Součást Light Agent je tak nainstalována na virtuální počítač. Můžete použít rozhraní aplikace a v oznamovací oblasti se zobrazí ikona aplikace . Nyní musíte nakonfigurovat připojení součásti Light Agent k SVM.



Hlavní okno součásti Light Agent

Připojování součásti Light Agent k SVM

Řešení Kaspersky Security for Virtualization Light Agent vyžaduje nepřetržitou komunikaci součásti Light Agent a SVM. Je to nutné kvůli kontrole souborů odesílaných součástí Light Agent na kontrolu výskytu virů a jiného malwaru. Bez připojení SVM nemůže Light Agent posílat soubory ke kontrole. Pokud připojení nelze navázat déle než pět minut, kontrola skončí chybou.

Připojení součásti Light Agent k SVM zahrnuje následující kroky:

1. Light Agent načte seznam dostupných modulů SVM.
2. Light Agent určí dostupný server pro ochranu (SVM), který je optimální pro připojení na základě algoritmu výběru SVM.
3. Light Agent zkontroluje další nastavení připojení SVM: značky, stav ochrany připojení, funkce aplikace, na které se vztahuje licence.
4. Připojování součásti Light Agent k SVM.

Informace o stavu připojení součásti Light Agent k SVM můžete získat v aplikaci Kaspersky Endpoint Security nebo pomocí příkazu aplikace. Aplikace vygeneruje událost při každé ztrátě nebo navázání připojení součásti Light Agent k SVM a odešle tyto události do aplikace Kaspersky Security Center. Pokud pro zjišťování SVM používáte integrační server, můžete informace o stavu SVM a počtu připojených součástí Light Agents získat v konzole integračního serveru. Podrobnosti o sledování stavu SVM najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

Zjištění SVM

Pro součást Light Agent můžete vybrat jednu z metod zjišťování SVM:

- Pomocí integračního serveru (VIIS).

  Integrační server je součást řešení, která umožňuje interakci řešení Kaspersky Security for Virtualization Light Agent s virtuální infrastrukturou. Integrační server spravuje seznam serverů SVM, ke kterým se lze připojit. Light Agent naváže připojení k integračnímu serveru a získá seznam adres SVM.

  Integrační server je užitečný ve velkých virtuálních infrastrukturách, protože automaticky vyrovnává zátěž mezi servery SVM. Integrační server získá informace o dostupných SVM, analyzuje je a poskytne součástem Light Agent seznam serverů pro ochranu (SVM), které jsou optimální pro připojení.

  Aby součást Light Agent mohla získat seznam SVM, stačí zadat adresu integračního serveru.

- Používání seznamu adres SVM.

  Pokud potřebujete určit jednotlivé servery SVM, ke kterým chcete součást Light Agent připojovat, můžete seznam připravit ručně.

  Je třeba uvést adresy dostupných serverů SVM, ke kterým se může součást Light Agent připojit.

Jak nakonfigurovat zjišťování SVM pomocí součásti Light Agent v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Režim Light Agent** → **Nastavení zjišťování SVM**.
4. Vyberte metodu zjišťování SVM.
   - **Používat integrační server**. Zadejte nastavení připojení k integračnímu serveru. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) zařízení, na kterém je nainstalován integrační server.
   - **Používat vlastní seznam adres SVM**. Vytvořte seznam SVM, ke kterým se může Light Agent připojit. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) SVM. Každou položku seznamu je třeba zadat na nový řádek nebo oddělit od předchozí položky středníkem (`;`).

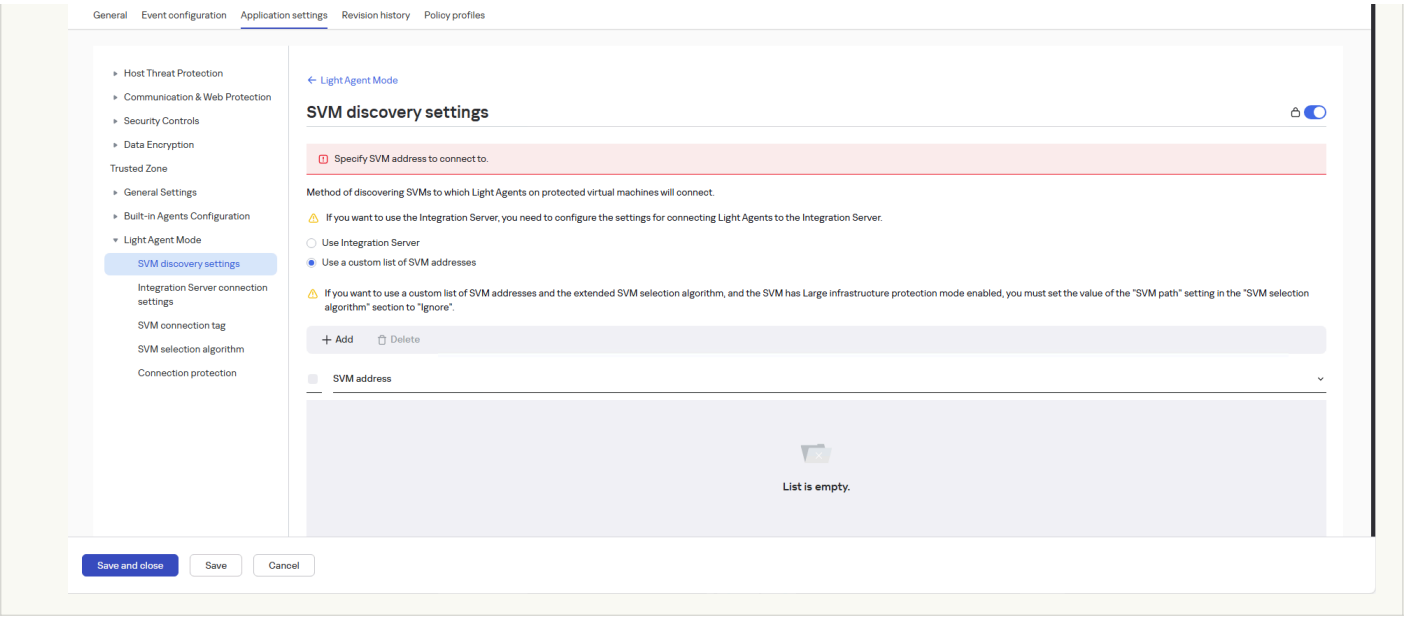
     V seznamu adres SVM zadejte pouze plně kvalifikované názvy domén (FQDN), které odpovídají jedné IP adrese. Použití plně kvalifikovaného názvu domény, který odpovídá více IP adresám, může vést k chybám v řešení.
5. Uložte změny.

Jak nakonfigurovat zjišťování SVM pomocí součásti Light Agent ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Light Agent Mode** → **SVM discovery settings**.
5. Vyberte metodu zjišťování SVM.
   - **Use Integration Server**. Zadejte nastavení připojení k integračnímu serveru. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) zařízení, na kterém je nainstalován integrační server.
   - **Use a custom list of SVM addresses**. Vytvořte seznam SVM, ke kterým se může Light Agent připojit. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) SVM. Každou položku seznamu je třeba zadat na nový řádek nebo oddělit od předchozí položky středníkem (`;`).

     V seznamu adres SVM zadejte pouze plně kvalifikované názvy domén (FQDN), které odpovídají jedné IP adrese. Použití plně kvalifikovaného názvu domény, který odpovídá více IP adresám, může vést k chybám v řešení.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.



Jak nakonfigurovat zjišťování SVM pomocí součásti Light Agent v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace v části **Režim Light Agent** klikněte na dlaždici **Nastavení zjišťování SVM**.
3. Vyberte metodu zjišťování SVM.
   - **Používat integrační server**. Zadejte nastavení připojení k integračnímu serveru. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) zařízení, na kterém je nainstalován integrační server.
   - **Používat vlastní seznam adres SVM**. Vytvořte seznam SVM, ke kterým se může Light Agent připojit. Zadejte IP adresu ve formátu IPv4 nebo plně kvalifikovaný název domény (FQDN) SVM. Každou položku seznamu je třeba zadat na nový řádek nebo oddělit od předchozí položky středníkem (**;**).

     V seznamu adres SVM zadejte pouze plně kvalifikované názvy domén (FQDN), které odpovídají jedné IP adrese. Použití plně kvalifikovaného názvu domény, který odpovídá více IP adresám, může vést k chybám v řešení.
4. Uložte změny.

Konfigurace algoritmu výběru SVM pro součást Light Agent

Infrastruktura organizace může mít více nasazených serverů SVM, ke kterým se mohou součásti Light Agent připojovat. Chcete-li vyvážit zatížení sítě a prostředků virtuální infrastruktury, musíte distribuovat součásti Light Agenty mezi servery SVM.

Součásti Light Agent mohou pro připojení použít jeden z následujících algoritmů výběru SVM:

- **Standardní algoritmus** (ve výchozím nastavení)

  Standardní algoritmus zahrnuje následující kroky:

  1. Light Agent identifikuje *místní SVM*.

     K identifikaci serveru SVM jako místního používá Light Agent hlavně jeho umístění ve virtuální infrastruktuře. Pokud jsou servery SVM umístěny ve stejném hypervizoru jako součást Light Agent, považuje je součást Light Agent za místní. V některých virtuálních infrastrukturách musíte ručně určit místní servery SVM pomocí konfiguračního souboru.

  2. Pokud Light Agent detekuje více místních serverů SVM, Light Agent vybere SVM s nejmenším počtem připojených součástí Light Agent. Pokud se vám nepodařilo identifikovat místní servery SVM, Light Agent vybere SVM s nejmenším počtem připojených součástí Light Agent v celé virtuální infrastruktuře.

  Podrobnosti o místních serverech SVM najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

- **Rozšířený algoritmus**

Rozšířený algoritmus umožňuje ručně určit místní kritéria výběru serveru SVM nebo zakázat zjišťování místních serverů SVM. Chcete-li tak učinit, musíte vybrat cestu k SVM ve virtuální infrastruktuře: hypervizor, cluster nebo datové centrum. To znamená, že musíte vybrat rozsah, ve kterém mají být místní servery SVM zjišťovány. Pokud se součást Light Agent nemůže připojit k místnímu SVM v nakonfigurovaném rozsahu zjišťování, přestane se pokoušet o připojení. Rozšířený algoritmus také umožňuje u součásti Light Agent zakázat místní zjišťování SVM. V tomto případě Light Agent vybere SVM s nejmenším počtem připojených součástí Light Agent v celé virtuální infrastruktuře.

Kromě algoritmů připojení k SVM můžete regulovat připojování součástí Light Agent k serverům SVM pomocí značek.

Jak nakonfigurovat algoritmus výběru SVM u součásti Light Agent v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Režim Light Agent** → **Algoritmus výběru SVM**.
4. Vyberte algoritmus:
   - **Používat standardní algoritmus výběru SVM**. Light Agent vybere servery SVM nasazené ve stejném hypervizoru.
   - **Používat rozšířený algoritmus výběru SVM**. Light Agent vybere servery SVM nasazené ve vybraném typu cesty k SVM (ve výchozím nastavení **Hypervizor**).
5. V případě potřeby vyberte cestu k SVM pro rozšířený algoritmus výběru SVM:
   - **Hypervizor**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném hypervizoru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - SVM je umístěn ve stejné skupině serverů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném hypervizoru nebo ve stejné skupině serverů, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.
   - **Cluster**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném clusteru hypervizorů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM jsou nasazeny ve stejném projektu OpenStack jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném clusteru hypervizorů nebo ve stejném projektu OpenStack, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.
   - **Datové centrum**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném datovém centru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM se nacházejí ve stejné zóně dostupnosti jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud ve stejném datovém centru nebo zóně dostupnosti, kde se nachází virtuální počítač se součástí Light Agent, nejsou k dispozici žádné SVM pro připojení, Light Agent se k SVM nepřipojí.
   - **Ignorovat**. Light Agent ignoruje cestu k SVM pro připojení k serveru pro ochranu. Součást Light Agent bere v úvahu další kritéria: značky, počet součástí Light Agent připojených k SVM atd.
6. Uložte změny.

Jak nakonfigurovat algoritmus výběru SVM u součásti Light Agent ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Light Agent Mode → SVM selection algorithm**.

5. Vyberte algoritmus:

   - **Use the standard SVM selection algorithm**. Light Agent vybere servery SVM nasazené ve stejném hypervizoru.
   - **Use the extended SVM selection algorithm**. Light Agent vybere servery SVM nasazené ve vybraném typu cesty k SVM (ve výchozím nastavení **Hypervisor**).

6. V případě potřeby vyberte cestu k SVM pro rozšířený algoritmus výběru SVM:

   - **Hypervisor**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):

     - Servery SVM jsou nasazeny ve stejném hypervizoru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - SVM je umístěn ve stejné skupině serverů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném hypervizoru nebo ve stejné skupině serverů, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.

   - **Cluster**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):

     - Servery SVM jsou nasazeny ve stejném clusteru hypervizorů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM jsou nasazeny ve stejném projektu OpenStack jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném clusteru hypervizorů nebo ve stejném projektu OpenStack, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.

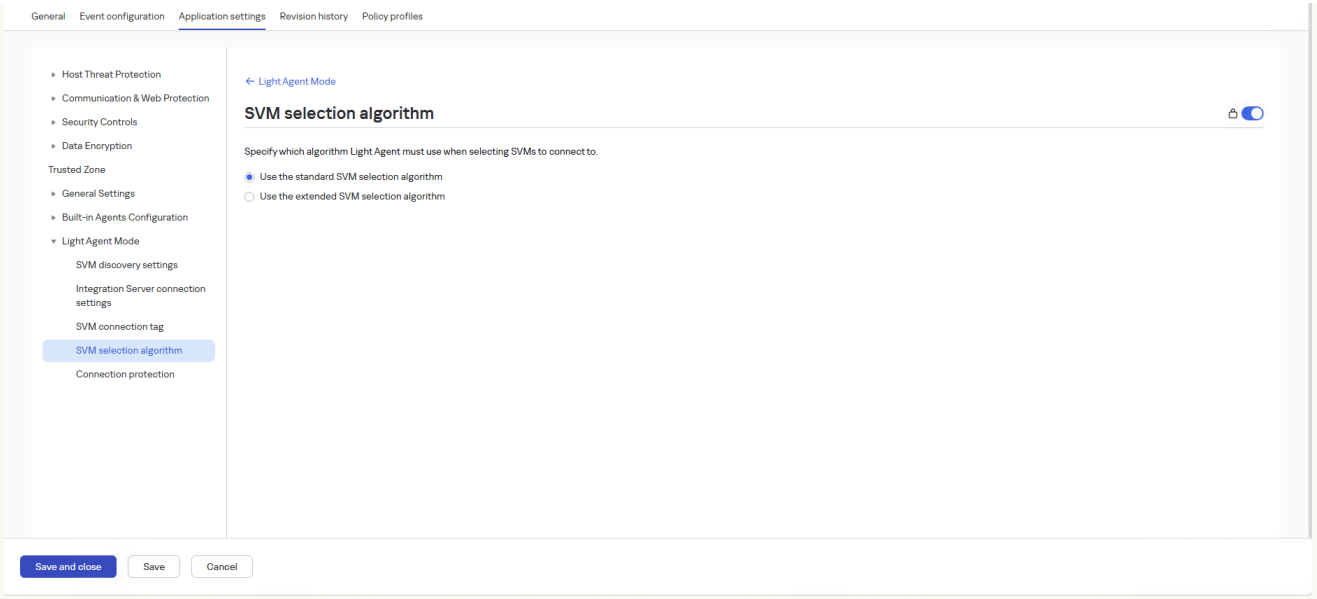
   - **Data center**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):

     - Servery SVM jsou nasazeny ve stejném datovém centru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM se nacházejí ve stejné zóně dostupnosti jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud ve stejném datovém centru nebo zóně dostupnosti, kde se nachází virtuální počítač se součástí Light Agent, nejsou k dispozici žádné SVM pro připojení, Light Agent se k SVM nepřipojí.

   - **Ignore**. Light Agent ignoruje cestu k SVM pro připojení k serveru pro ochranu. Součást Light Agent bere v úvahu další kritéria: značky, počet součástí Light Agent připojených k SVM atd.

7. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.



Oddíl zásad algoritmu výběru SVM

Jak nakonfigurovat algoritmus výběru SVM u součásti Light Agent v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace v části **Režim Light Agent** klikněte na dlaždici **Nastavení zjišťování SVM**.
3. Vyberte algoritmus:
   - **Používat standardní algoritmus výběru SVM**. Light Agent vybere servery SVM nasazené ve stejném hypervizoru.
   - **Používat rozšířený algoritmus výběru SVM**. Light Agent vybere servery SVM nasazené ve vybraném typu cesty k SVM (ve výchozím nastavení **Hypervizor**).
4. V případě potřeby vyberte cestu k SVM pro rozšířený algoritmus výběru SVM:
   - **Hypervizor**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném hypervizoru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - SVM je umístěn ve stejné skupině serverů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném hypervizoru nebo ve stejné skupině serverů, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.
   - **Cluster**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném clusteru hypervizorů jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM jsou nasazeny ve stejném projektu OpenStack jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

     Pokud na stejném clusteru hypervizorů nebo ve stejném projektu OpenStack, kde je umístěn virtuální počítač se součástí Light Agent, nejsou žádné dostupné servery SVM, pak se Light Agent k SVM nepřipojí.
   - **Datové centrum**. Light Agent vybere pro připojení server SVM, který odpovídá konkrétnímu kritériu (v závislosti na typu virtuální infrastruktury):
     - Servery SVM jsou nasazeny ve stejném datovém centru jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře na serverech Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux nebo Numa vServer).
     - Servery SVM se nacházejí ve stejné zóně dostupnosti jako virtuální počítač s nainstalovanou součástí Light Agent (ve virtuální infrastruktuře spuštěné na platformě OpenStack, VK Cloud nebo TIONIX Cloud Platform).

Pokud ve stejném datovém centru nebo zóně dostupnosti, kde se nachází virtuální počítač se součástí Light Agent, nejsou k dispozici žádné SVM pro připojení, Light Agent se k SVM nepřipojí.

- **Ignorovat**. Light Agent ignoruje cestu k SVM pro připojení k serveru pro ochranu. Součást Light Agent bere v úvahu další kritéria: značky, počet součástí Light Agent připojených k SVM atd.

5. Uložte změny.

Distribuce připojení součástí Light Agent k součástem SVM (značky)

K SVM se může připojit více součástí Light Agent. Chcete-li vyvážit připojení součásti Light Agent, můžete zadat samostatný seznam SVM. Pokud používáte integrační server pro zjišťování SVM, můžete použít *značky* k vyvážení připojení součásti Light Agent k modulům SVM. To znamená, že součásti Light Agent můžete přiřadit seznam SVM pro připojení pomocí značky. Chcete-li tak učinit, musíte k součásti Light Agent přiřadit značku a tuto značku určit v nastavení SVM. Podrobnosti o určení značek v nastavení součásti SVM najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

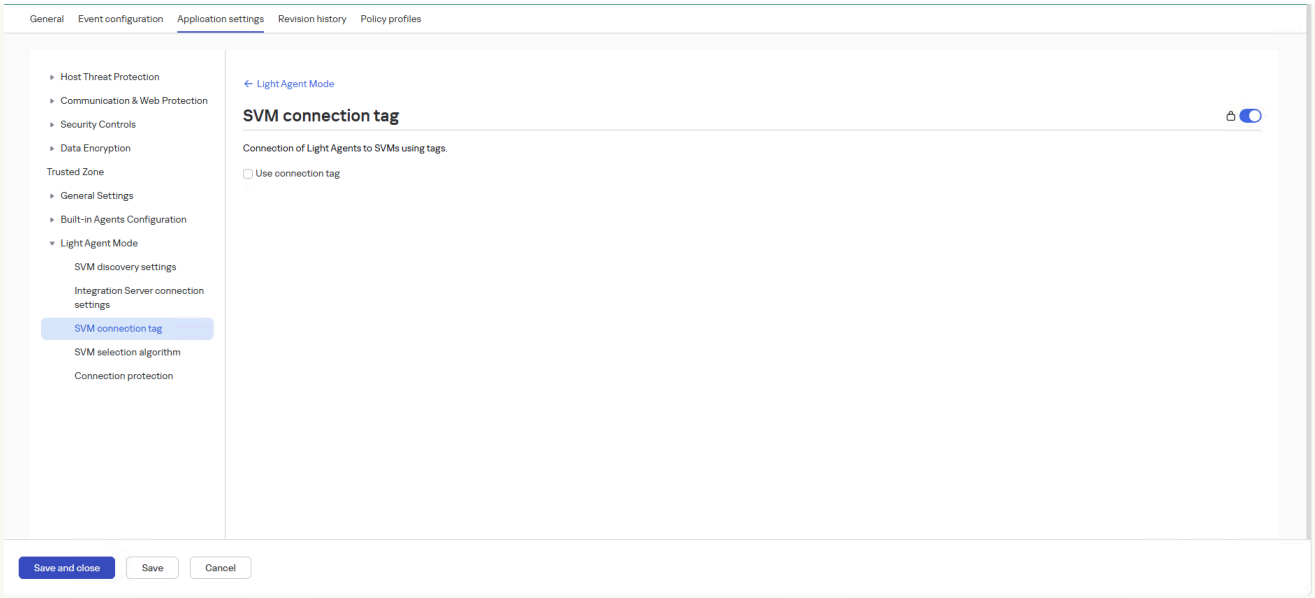
Příklad: Řešení Kaspersky Endpoint Detection and Response Optimum je nasazeno do vaší infrastruktury pro určené hostitele virtuálních strojů. V tomto případě můžete součásti Light Agent přiřadit značku `[EDROptimum]`, aby se připojovala k serverům SVM, které mají přidaný licenční klíč EDR Optimum (doplněk EDR Optimum). Díky tomu můžete na virtuálním počítači se součástí Light Agent používat funkce EDR Optimum. Při připojování součásti Light Agent k SVM bez licenčního klíče k EDR Optimum nebudou funkce Kaspersky Endpoint Detection and Response Optimum dostupné.

Jak přiřadit značku připojení SVM k součásti Light Agent v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Režim Light Agent** → **Značka připojení SVM**.
4. Zaškrtněte políčko **Použít značku připojení** a zadejte značku připojení k SVM.
   U značky můžete zadat textový řetězec dlouhý až 255 znaků. Můžete použít libovolný znak kromě znaku `;`.
5. Uložte změny.

Jak přiřadit značku připojení SVM k součásti Light Agent ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **Light Agent Mode** → **SVM connection tag**.
5. Zaškrtněte políčko **Use connection tag** a zadejte značku připojení k SVM.
   U značky můžete zadat textový řetězec dlouhý až 255 znaků. Můžete použít libovolný znak kromě znaku `;`.
6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.



Připojování k části zásad pro značky KUMA

Jak přiřadit značku připojení SVM k součásti Light Agent v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace v části **Režim Light Agent** klikněte na dlaždici **Značka připojení SVM**.
3. Zaškrtněte políčko **Použít značku připojení** a zadejte značku připojení k SVM.
   U značky můžete zadat textový řetězec dlouhý až 255 znaků. Můžete použít libovolný znak kromě znaku `;`.
4. Uložte změny.

Ochrana připojení mezi součástí Light Agent a SVM

Můžete nakonfigurovat šifrování připojení mezi součástmi Light Agent a serverem pro ochranu. Chcete-li to provést, musíte povolit šifrování datového kanálu mezi součástí Light Agent a serverem pro ochranu v nastavení serveru pro ochranu na SVM a v nastavení součásti Light Agent.

Součást Light Agent, u které je povolena ochrana připojení, se může připojovat pouze k serverům SVM, u nichž je povoleno šifrování datového kanálu mezi součástí Light Agent a serverem pro ochranu. Součást Light Agent, u které je zakázána ochrana připojení, se může připojovat pouze k serverům SVM, u nichž je zakázáno šifrování kanálu nebo je povoleno nezabezpečené připojení mezi serverem pro ochranu a součástí Light Agent.

Podrobnosti o konfiguraci ochrany připojení na serveru pro ochranu najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

Ochrana připojení pomocí šifrování může mít vliv na výkon součásti Kaspersky Security for Virtualization Light Agent.

Jak nakonfigurovat ochranu připojení v součásti Light Agent v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Režim Light Agent** → **Ochrana připojení**.
4. Zaškrtněte políčko **Šifrování datového kanálu mezi agentem Light Agent a serverem pro ochranu**.
5. Uložte změny.

Jak nakonfigurovat ochranu připojení v součásti Light Agent ve webové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

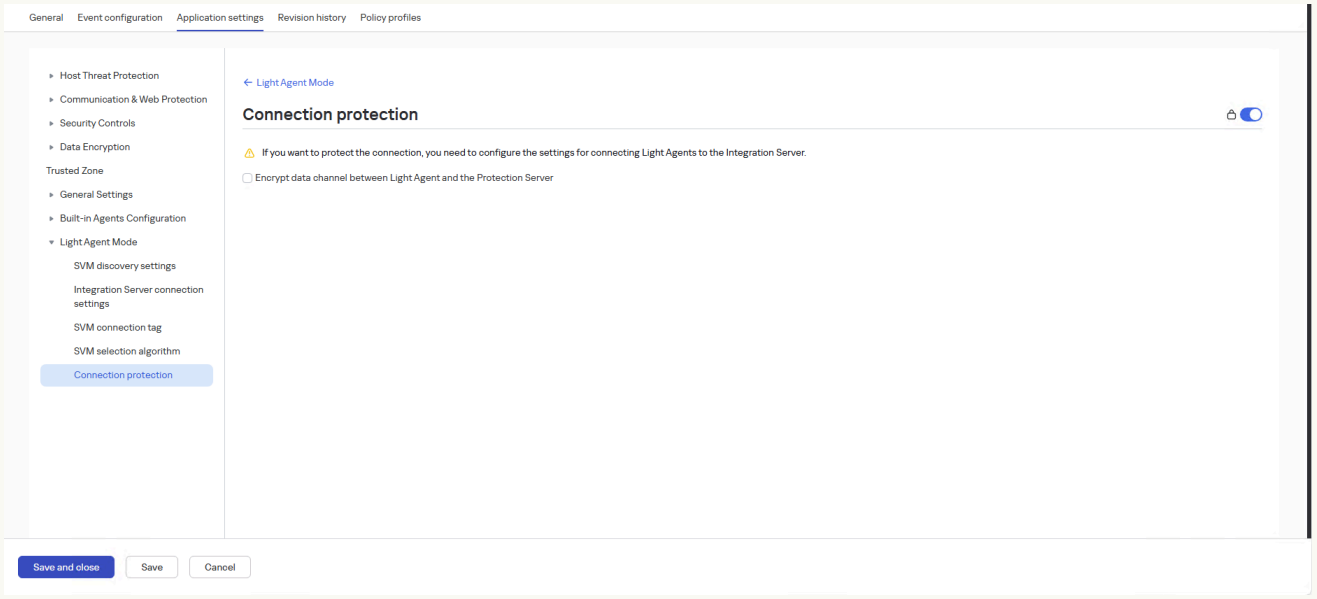
   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **Light Agent Mode → Connection protection**.

5. Zaškrtněte políčko **Encrypt data channel between Light Agent and the Protection Server**.

6. Chcete-li zásady použít na počítače, zavřete soubor ikony visacího zámku a uložte změny.



Oddíl zásad ochrany připojení

Jak nakonfigurovat ochranu připojení v součásti Light Agent v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko .

2. V okně nastavení aplikace v části **Režim Light Agent** klikněte na dlaždici **Ochrana připojení**.

3. Zaškrtněte políčko **Šifrování datového kanálu mezi agentem Light Agent a serverem pro ochranu**.

4. Uložte změny.

Aktivace součásti Light Agent

Pokud se aplikace Kaspersky Endpoint Security používá v režimu Light Agent pro ochranu virtuálních prostředí, není nutné aplikaci aktivovat samostatně. Pro aktivaci aplikace musíte na SVM přidat licenční klíč. Licenční klíč k SVM můžete přidat pomocí zvláštní úlohy v konzole aplikace Kaspersky Security Center. V rozhraní Light Agent nelze spravovat licenční klíče, můžete si však prohlédnout informace o licenci (viz obrázek níže). Informace o licenci k součásti Light Agent můžete také zobrazit z příkazového řádku (viz pokyny níže). Light Agent tyto informace získává od SVM. Podrobnosti o aktivaci řešení a správě licenčních klíčů najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

Postup zobrazení informací o licenci k součásti Light Agent:

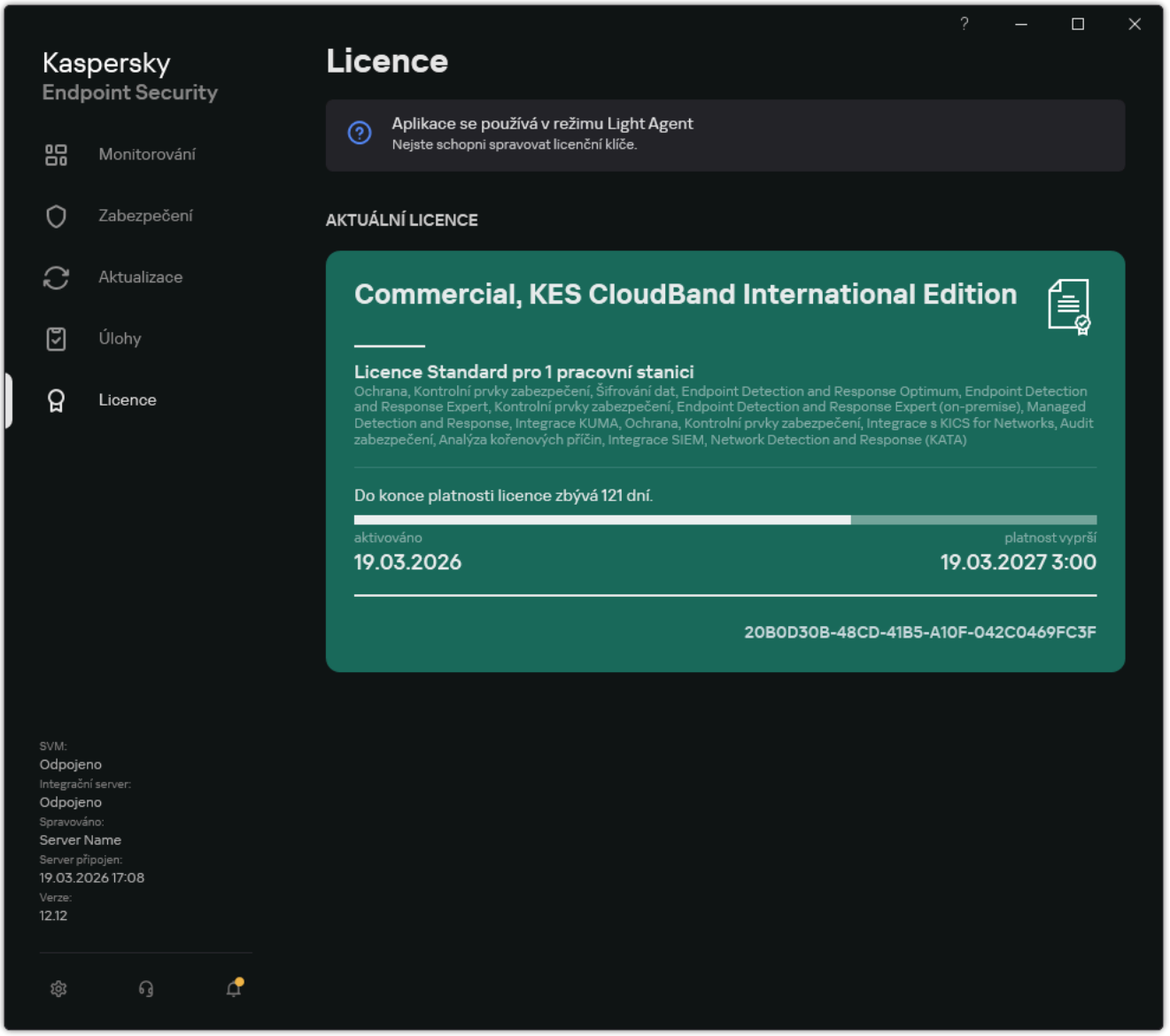
1. Spusťte překladač příkazového řádku (cmd) jako správce.

2. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

3. Spusťte následující příkaz:

   avp.com LICENSE /CHECK

Aplikace Kaspersky Endpoint Security tak zobrazuje informace o licenci: adresu SVM, ke kterému je součást Light Agent připojena, počet dní do vypršení platnosti licence a další informace. Pokud při aktivaci součásti Light Agent narazíte na nějaké problémy, nahlédněte do znalostní databáze technické podpory.



Okno Správa licence

Příručka migrace součásti KSVLA Light Agent na KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent zahrnuje součást Light Agent pro systém Windows 5.2 (dále také „KSVLA Light Agent“). V součásti Kaspersky Security for Virtualization Light Agent 6.2 se jako součást Light Agent používá Kaspersky Endpoint Security v režimu Light Agent. Chcete-li aktualizovat řešení na verzi 6.2, musíte migrovat ze součásti KSVLA Light Agent 5.2 na aplikaci Kaspersky Endpoint Security v režimu Light Agent (dále také „KES Light Agent“). Podrobnosti o aktualizaci verze řešení Kaspersky Security for Virtualization Light Agent najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

Požadavky na software

Před zahájením migrace ze součásti KSVLA Light Agent na KES Light Agent se ujistěte, že váš server splňuje požadavky aplikace Kaspersky Endpoint Security pro systém Windows na hardware a software. Seznamy podporovaných verzí operačního systému se pro KES a KSWS liší. KES například nepodporuje servery se systémem Windows Server 2003.

Minimální požadavky na software pro migraci z KSVLA Light Agent na KES Light Agent:

- Kaspersky Endpoint Security pro systém Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (včetně součástí Server pro ochranu a Integrační server).
- Kaspersky Security Center 14.2

  Pokud máte nainstalovanou starší verzi aplikace Kaspersky Security Center, aktualizujte ji na verzi 14.2 nebo novější. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh umožňuje migrovat zásady do profilu, nikoli do zásady. V této verzi aplikace Kaspersky Security Center vám průvodce hromadným převodem zásad a úloh také umožňuje migrovat širší rozsah nastavení zásad.

Kroky migrace

Migrace z KSVLA Light Agent na KES Light Agent se provádí poloautomaticky. To je nutné z důvodu rozdílných architektur aplikací.

Proveďte migraci z KSVLA Light Agent na KES Light Agent v následujícím pořadí:

1. **Proveďte migraci úloh a zásad KSVLA Light Agent**

   Chcete-li migrovat nastavení zásad, musíte spustit průvodce hromadným převodem zásad a úloh (průvodce migrací). Po migraci nastavení zásad musíte ručně nakonfigurovat nastavení, která průvodce migrací nemůže migrovat automaticky (například nastavení aktualizace databází). Po migraci je také doporučeno zkontrolovat, zda průvodce migrací správně migroval všechna nastavení.

   > Pokud je povolena Ochrana heslem za účelem omezení přístupu k součásti KSVLA Light Agent, před instalací součásti KES Light Agent musíte v zásadách součásti KSVLA Light Agent tuto funkci zakázat. V nastavení instalačního balíčku součásti KES Light Agent nelze heslo pro odinstalaci zadat. Po dokončení instalace součásti KES Light Agent přes KSVLA Light Agent musíte v zásadách KES povolit funkci Ochrana heslem.

2. **Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent**

   Součást KES Light Agent můžete nainstalovat následujícími způsoby:

   - Instalace součásti KES Light Agent po odebrání součásti KSVLA Light Agent (doporučeno)
   - Instalace součásti KES Light Agent přes součást KSVLA Light Agent

3. **Ověření, zda je aplikace po migraci funkční**

   Po migraci ze součásti KSVLA Light Agent na KES Light Agent se ujistěte, že aplikace funguje správně. Aktivujte převedené zásady. V konzole aplikace Kaspersky Security Center zkontrolujte stav virtuálního počítače (měl by být *OK*). Ujistěte se, že pro aplikaci nejsou hlášeny žádné chyby, zkontrolujte také čas posledního připojení k SVM a stav ochrany virtuálního počítače. Není nutné aktivovat součást Light Agent, protože licenční klíč se přidává na SVM.

Instalace součásti KES Light Agent namísto součásti KSVLA Light Agent

Součást KES Light Agent můžete nainstalovat následujícími způsoby:

- Instalace součásti KES Light Agent po odebrání součásti KSVLA Light Agent (doporučeno)
- Instalace součásti KES Light Agent přes součást KSVLA Light Agent

Odebírání součásti KSVLA Light Agent

Aplikaci můžete odebrat vzdáleně pomocí úlohy *Install application remotely*, místně na virtuálním počítači nebo v šabloně virtuálního počítače. Po odebrání součásti KSVLA Light Agent bude pravděpodobně nutné restartovat virtuální počítač.

Po odebrání součásti KSVLA Light Agent nainstalujte součásti KES Light Agent za použití jakékoliv vhodné metody.

Instalace aplikace Kaspersky Endpoint Security

> Pokud je povolena Ochrana heslem za účelem omezení přístupu k součásti KSVLA Light Agent, před instalací součásti KES Light Agent musíte v zásadách součásti KSVLA Light Agent tuto funkci zakázat. V nastavení instalačního balíčku součásti KES Light Agent nelze heslo pro odinstalaci zadat. Po dokončení instalace součásti KES Light Agent přes KSVLA Light Agent musíte v zásadách KES povolit funkci Ochrana heslem.

Při instalaci aplikace Kaspersky Endpoint Security musíte vybrat režim **Light Agent na ochranu virtuálních prostředí**. Před instalací součásti KES Light Agent na virtuálním počítači instalační program zjistí KSVLA Light Agent jako nekompatibilní software a odebere jej. Migrace konfigurace součásti KSVLA Light Agent není podporována. To znamená, že při instalaci součásti KES Light Agent je kombinace součástí, které chcete nainstalovat, určena vaším výběrem ve vlastnostech instalačního balíčku nebo v průvodci instalací. Po odebrání součásti KSVLA Light Agent musíte restartovat virtuální počítač.

Nastavení a úlohy součásti KSVLA Light Agent se při instalaci součásti KES Light Agent nemigrují. Chcete-li migrovat nastavení a úlohy, spusťte průvodce hromadným převodem zásad a úloh.

Seznam nainstalovaných součástí si můžete prohlédnout v části **Zabezpečení** v rozhraní aplikace pomocí příkazu `status` nebo v konzole aplikace Kaspersky Security Center ve vlastnostech počítače. Sadu součástí můžete po instalaci změnit pomocí úlohy *Změna součástí aplikace*.

Shoda součástí KSVLA Light Agent a KES Light Agent

Kombinace součástí KSVLA Light Agent a KES Light Agent KES jsou prakticky stejné. KES Light Agent má více nastavení než KSVLA Light Agent. Po migraci má nové nastavení výchozí hodnoty.

Shoda součástí KSVLA Light Agent a KES Light Agent

Light Agent 5.2	KES Light Agent

Scan kernel	Jádro aplikace
File Anti-Virus	Ochrana před souborovými hrozbami
Mail Anti-Virus	Ochrana před hrozbami v poště
Web Anti-Virus	Ochrana před webovými hrozbami
Firewall	Brána firewall
Network Attack Blocker	Ochrana před síťovými hrozbami
Application Privilege Control	Prevence narušení hostitele
Applications Launch Control	Kontrola aplikací
Web Control	Kontrola webu
Device Control	Kontrola zařízení
System Watcher	V aplikaci Kaspersky Endpoint Security je tato součást rozdělena na následující součásti: • Prevence zneužití • Detekce chování • Modul pro nápravu
System Integrity Monitoring	Monitorování integrity systému
Integration with Kaspersky Endpoint Agent	*(není podporováno)* V aplikaci Kaspersky Endpoint Security od verze 11.9.0 již není distribuční balíček Kaspersky Endpoint Agent součástí distribuční sady.
AMSI Protection	Ochrana AMSI

Migrace úloh a zásad součásti KSVLA Light Agent

Nastavení zásad a úloh součásti KSVLA Light Agent můžete migrovat pomocí průvodce hromadným převodem zásad a úloh (dále také „průvodce migrací").

Průvodce migrací pro KSVLA Light Agent je k dispozici pouze v konzole pro správu (MMC). Nastavení zásad a úloh nelze migrovat ve webové konzole a cloudové konzole.

Při migrací zásad a úloh je potřeba vzít v úvahu následující zvláštní aspekty:

- Nová zásada má název *<Zásady> (converted)*.
- Nová zásada má stav *Inactive policy*.
- Zákaz úprav nastavení („zámek") migrován není. Průvodce migrací nastaví výchozí hodnoty.
- Profily zásad se nemigrují. Profily zásad musíte přidat ručně.
- Byla vylepšena správa důvěryhodných zón. V součásti KSVLA Light Agent jste mohli přidat předdefinované výjimky pouze při vytváření zásad. Následně jste ve vlastnostech zásad mohli nakonfigurovat dříve přidané předdefinované výjimky nebo přidat výjimky ručně. Do vlastností zásad nelze přidávat předdefinované výjimky. V součásti KES Light Agent jsou předdefinované výjimky k dispozici během vytváření zásad i ve vlastnostech vytvořené zásady. Předdefinované výjimky můžete také vybrat v instalačním balíčku.
- Konfigurace uživatelského rozhraní aplikace v aplikaci Kaspersky Endpoint Security byla přesunuta z instalačního programu do zásad. Pokud potřebujete například skrýt uživatelské rozhraní aplikace, spravujte nastavení zásad.
- Sady funkcí pro konfiguraci kontroly přístupu založeného na právech (RBAC) se v aplikaci Kaspersky Endpoint Security a součásti KSVLA Light Agent liší. Přístupová práva uživatelů k funkčním oblastem musíte nakonfigurovat od začátku.

Jak pomocí průvodce hromadným převodem zásad a úloh migrovat nastavení zásad součásti KSVLA Light Agent

1. V konzole pro správu vyberte položku Administration Server a kliknutím pravým tlačítkem otevřete místní nabídku.
2. Vyberte **All tasks → Policies and tasks batch conversion wizard**.

Spustí se průvodce hromadným převodem zásad a úloh. Postupujte podle pokynů průvodce.

Krok 1. Výběr aplikace, pro kterou potřebujete převést zásady a úlohy

V tomto kroku musíte vybrat Kaspersky Endpoint Security pro systém Windows. Přejděte k dalšímu kroku.

Krok 2. Převod zásad

Vyberte zásady řešení Kaspersky Security for Virtualization 5.2 Light Agent pro systém Windows, které chcete převést. Přejděte k dalšímu kroku.

Průvodce migrací poté začne převádět zásady. Během převodu vás průvodce migrací vyzve, abyste přijali prohlášení o KSN. Nová zásada má název *<Zásady> (converted)*.

Krok 3. Převod úloh

Nové úlohy pro aplikaci Kaspersky Endpoint Security pro systém Windows vytvoří průvodce migrací. V seznamu úloh vyberte úlohy součásti KSVLA Light Agent, které chcete vytvořit pro zásady aplikace Kaspersky Endpoint Security. Nové úlohy budou mít název *<Název úlohy> (converted)*. Přejděte k dalšímu kroku.

Krok 4. Dokončení průvodce

Ukončete průvodce.

Po migraci zásady je třeba otevřít její vlastnosti, zkontrolovat její nastavení a uložit ji. Pokud tyto kroky neprovedete, může KES Light Agent převedenou zásadu ignorovat.

Zvláštní pozornost věnujte migraci nastavení připojení součásti Light Agent k SVM, seznamů výjimek, důvěryhodných aplikací, důvěryhodných webových adres a pravidel součásti Kontrola aplikací.

Migrace konfigurace [KSVLA Light Agent+KEA] na konfiguraci [KES Light Agent+integrovaný agent]

Pro podporu používání aplikace Kaspersky Endpoint Security pro systém Windows v rámci řešení EDR (KATA), EDR Optimum, Kaspersky Sandbox byl do aplikace přidán integrovaný agent. Pro práci s těmito řešeními už nepotřebujete samostatnou aplikaci Kaspersky Endpoint Agent.

Při migraci ze součásti KSVLA Light Agent na KES Light Agent budou řešení EDR (KATA), EDR Optimum, Kaspersky Sandbox nadále spolupracovat s aplikací Kaspersky Endpoint Security. Kromě toho bude z počítače odebrána aplikace Kaspersky Endpoint Agent.

Před migrací ze součásti KSVLA Light Agent na KES Light Agent musíte aktualizovat všechny součásti aplikace Kaspersky Security for Virtualization na verzi 6.2, včetně serveru pro ochranu a integračního serveru. Podrobnosti o aktualizaci verze řešení Kaspersky Security for Virtualization Light Agent najdete v nápovědě k řešení Kaspersky Security for Virtualization Light Agent.

Migrace konfigurace [KSVLA Light Agent+KEA] na konfiguraci [KES Light Agent+integrovaný agent] zahrnuje následující kroky:

1. **Migrace zásady a úkolů**

   Migrace zásad a úloh [KSVLA Light Agent+KEA] na [KES Light Agent+integrovaný agent] zahrnuje následující kroky:

   1. Migrace zásad a úloh ze součásti KSVLA Light Agent na KES Light Agent pomocí Průvodce hromadným převodem zásad a úloh (k dispozici pouze v konzole pro správu (MMC)).

      Je tak vytvořena nová zásada s názvem *<Zásada> (converted)*. Nové úlohy KES jsou také vytvářeny s názvy *<Název úlohy> (converted)*.

   2. Migrace zásad a úloh z KEA na KES pomocí průvodce migrací z aplikace Kaspersky Endpoint Agent (k dispozici pouze ve webové konzole a cloudové konzole).

      Výsledkem je vytvoření nové zásady s názvem *<název zásady aplikace Kaspersky Endpoint Security> & <název zásady aplikace Kaspersky Endpoint Agent>*. Vytvářejí se také nové úlohy a úlohy KES.

2. **Migrace z KSVLA Light Agent na KES Light Agent**

   Migrace z KSVLA Light Agent na KES Light Agent zahrnuje instalaci KES Light Agent místo KSVLA Light Agent.

   Správci obvykle povolují ochranu heslem, aby omezili přístup k KSVLA Light Agent a KEA. Heslo pro odinstalaci KEA můžete zadat pouze ve vlastnostech úlohy *Install application remotely*. Před migrací musíte pro aplikaci KSVLA Light Agent zakázat Ochranu heslem.

Chcete-li provést migraci, musíte vybrat součásti potřebné pro podporu řešení Detection and Response jako součást aplikace Kaspersky Endpoint Security. Po instalaci se aplikace Kaspersky Endpoint Security přepne na používání integrovaného agenta a odebere aplikaci Kaspersky Endpoint Agent.

3. **Jak funguje licence**

   Pokud se aplikace používá v režimu Light Agent, není nutné aplikaci aktivovat samostatně. Pro aktivaci aplikace musíte na SVM přidat licenční klíč. Na SVM musíte také přidat licenční klíč pro aktivaci dalších funkcí (například EDR Optimum). To znamená, že v rámci migrace dochází k licencování funkcí automaticky.

4. **Kontrola stavu řešení Kaspersky Endpoint Detection and Response Optimum a Kaspersky Sandbox**

   Pokud je po upgradu stav počítače v konzole aplikace Kaspersky Security Center *Critical*:

   - Zkontrolujte, zda je v počítači nainstalována součást Network Agent verze 13.2 nebo novější.
   - Provozní stav integrovaného agenta zkontrolujete zobrazením *Report on status of application components*. Pokud má příslušná součást stav *Not installed* nainstalujte ji pomoc úlohy *Change application components*.
   - V nové zásadě aplikace Kaspersky Endpoint Security pro systém Windows musíte přijmout Prohlášení o Kaspersky Security Network.
   - Pomocí *Report on status of application components* zkontrolujte, zda je aktivována funkce EDR Optimum. Pokud je stav součásti *Není součástí licence*, zkontrolujte, zda je u EDR Optimum zapnuta funkce automatické distribuce licenčního klíče.
   - Zkontrolujte stav připojení virtuálního počítače k SVM. Informace o stavu připojení součásti Light Agent k SVM můžete získat v aplikaci Kaspersky Endpoint Security nebo pomocí příkazu aplikace.

Správa aplikace z příkazového řádku

Aplikaci Kaspersky Endpoint Security můžete spravovat z příkazového řádku. Seznam příkazů pro správu aplikace můžete zobrazit provedení příkazu `avp.com HELP`. Chcete-li si přečíst syntaxi konkrétního příkazu, zadejte `avp.com HELP <command>`.

Zvláštní znaky v příkazu je nutno escapovat. Chcete-li escapovat znaky `&`, `|`, `(`, `)`, `<`, `>`, `^`, použijte znak `^` (například pokud chcete použít znak `&`, zadejte `^&`). Pro escapování znaku `%` zadejte `%%`.

Místo hodnoty `1` lze použít hodnoty `yes`, `on`, `enable`, `enabled` a `true`. Místo hodnoty `0` lze použít hodnoty `no`, `off`, `disable`, `disabled` a `false`.

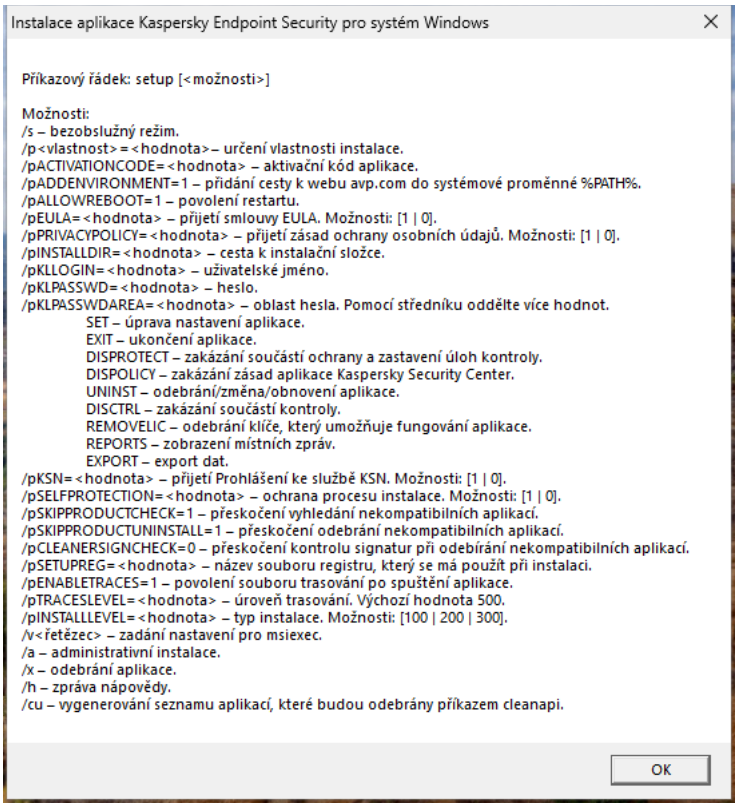
Setup. Instalace aplikace

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 (bezobslužná instalace). 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.

Seznam příkazů pro instalaci aplikace můžete zobrazit provedení příkazu `/h`. Chcete-li získat nápovědu k syntaxi instalačního příkazu, zadejte `setup_kes.exe /h`. Instalační program zobrazí okno s popisem možností příkazu (viz obrázek níže).



Popis možností instalačního příkazu

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] [/pCONFIGPATH=<path to the configuration file>] [/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>] [/pSKIPKB5007186CHECK=1] [/s]

   nebo

   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]

Aplikace je nainstalována na počítači. Potvrdit, zda je aplikace nainstalována, a zkontrolovat nastavení aplikace, můžete vydáním příkazu `status`.

Nastavení instalace aplikace

`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.

`CONFIGPATH=<path to the configuration file>`

Instalace aplikace s předdefinovaným nastavením. K tomu musíte nahrát soubor, který definuje nastavení aplikace Kaspersky Endpoint Security. Můžete vytvořit konfigurační soubor v místním rozhraní aplikace.

`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`

Zakáže kontrolu nainstalovaného softwaru. Seznam softwaru, který může způsobovat problémy s kompatibilitou, je k dispozici v souboru incompatible.txt, který je součástí distribuční sady. Pokud není u tohoto parametru nastavena žádná hodnota a je zjištěn software ze seznamu, instalace aplikace Kaspersky Endpoint Security bude ukončena.

`SKIPPRODUCTUNINSTALL=1`

Zakáže automatické odstranění zjištěného softwaru ze seznamu incompatible.txt. Pokud není u tohoto parametru nastavena žádná hodnota, aplikace Kaspersky Endpoint Security se pokusí software, který může způsobovat problémy s kompatibilitou, odebrat.

> Automatické odstranění softwaru nelze povolit, pokud instalujete Kaspersky Endpoint Security pomocí instalačního programu msiexec. Chcete-li automaticky odebrat software, který může způsobovat problémy s kompatibilitou, použijte soubor setup_kes.exe.

`CLEANERSIGNCHECK=0|1`

Ověřování digitálních podpisů zjištěných souborů softwaru ze seznamu incompatible.txt. Chcete-li software odebrat, Kaspersky Endpoint Security spustí instalační soubor softwaru. Pokud instalační soubor nemá digitální podpis, aplikace Kaspersky Endpoint Security považuje soubor za nedůvěryhodný a zastaví odstraňování softwaru, aby se zabránilo spuštění potenciálně škodlivého kódu. Pokud aplikace nemůže ověřit digitální podpis zjištěného souboru softwaru, instalace aplikace Kaspersky Endpoint Security se zastaví s chybou.

Výchozí hodnota se liší v závislosti na způsobu instalace softwaru:

- `0` znamená, že ověřování digitálního podpisu je zakázáno (výchozí hodnota, pokud je aplikace nasazována prostřednictvím Kaspersky Security Center).
- `1` znamená, že je povoleno ověřování digitálního podpisu (výchozí hodnota, pokud se aplikace instaluje lokálně).

`STANDALONEMODE=1`

Instalace aplikace v konfiguraci Endpoint Detection and Response Agent (EDR Agent) pro integraci s řešeními Kaspersky Endpoint Detection and Response (KATA) nebo Kaspersky Endpoint Detection and Response Expert (on-premise). Tato konfigurace je nutná, pokud je ve vaší organizaci spolu s řešením na úrovni Kaspersky Endpoint Detection and Response nasazena platforma Endpoint Protection Platform (EPP) třetí strany. Díky tomu je Kaspersky Endpoint Security v konfiguraci agenta Endpoint Detection and Response Agent kompatibilní s aplikacemi EPP třetích stran.

`KLLOGIN`

Nastavte uživatelské jméno pro přístup k funkcím a nastavením aplikace Kaspersky Endpoint Security (součást Ochrana heslem). Uživatelské jméno se nastavuje společně s nastaveními `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.
- `EXPORT` – export nastavení aplikace.

Například `KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT`.

Účet KLAdmin má právo provést jakoukoli akci, která je chráněna heslem. Konfigurace rozsahu hesel pro účet KLAdmin je tedy nemožná. Pokud se pokusíte nakonfigurovat rozsah hesel pro účet KLAdmin, aplikace zakáže zadané akce pro skupinu „Všichni".

`PROTECTOSSERVICES`

Ochrana funkce služeb operačního systému. Ochrana služeb operačního systému brání aplikacím třetích stran v narušení provozu služeb operačního systému. Mezi takové služby patří například služba automatického spouštění aplikace.

- `1` znamená, že je ochrana služeb operačního systému povolena (výchozí hodnota).
- `0` znamená, že je ochrana služeb operačního systému zakázána.

`ENABLETRACES`

Povolí nebo zakáže trasování aplikací. Po spuštění uloží aplikace Kaspersky Endpoint Security soubory trasování do složky `%ProgramData%\Kaspersky Lab\KES.14.0\Traces`. Dostupné hodnoty:

- `1` – trasování aplikací je povoleno.
- `0` – trasování aplikací je zakázáno (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.

`ENABLEAZURESUPPORT`

Povolení nebo zakázání režimu kompatibility Azure WVD. Dostupné hodnoty:

- `1` – Režim kompatibility Azure WVD je povolen.
- `0` – Režim kompatibility Azure WVD je zakázán (výchozí hodnota).

Tato funkce zajišťuje správné zobrazení stavu virtuálního počítače Azure v konzole Kaspersky Anti Targeted Attack Platform. Pro sledování výkonu počítače odesílá Kaspersky Endpoint Security telemetrii na servery KATA. Telemetrie zahrnuje ID počítače (Sensor ID). Režim kompatibility Azure WVD umožňuje těmto virtuálním počítačům přiřadit trvalé jedinečné Sensor ID. Pokud je režim kompatibility vypnutý, Sensor ID se může po restartování počítače změnit kvůli tomu, jak fungují virtuální počítače Azure. To může způsobit, že se na konzole objeví duplikáty virtuálních počítačů.

`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.

`UPGRADEMODE`

Režim upgradu aplikace:

- `Seamless` znamená upgrade aplikace s restartem počítače (výchozí hodnota).
- `Force` znamená upgrade aplikace bez restartování.

Aplikaci můžete upgradovat bez restartu od verze 11.10.0. Chcete-li upgradovat starší verzi aplikace, musíte restartovat počítač. Od verze 11.11.0 můžete bez restartování rovněž instalovat bezpečnostní opravy.

Při instalaci aplikace Kaspersky Endpoint Security není vyžadováno restartování. Režim upgradu aplikace bude tedy určen v nastavení aplikace. Tento parametr můžete změnit v nastavení aplikace nebo v zásadách.

Při upgradu již nainstalované aplikace je priorita parametru příkazového řádku nižší než priorita parametru uvedeného v nastavení aplikace nebo v souboru setup.ini. Například pokud je v příkazovém řádku zadán režim upgradu `Force` a v nastavení aplikace je zadán režim `Seamless`, upgrade se nainstaluje po restartu počítače (`Seamless`).

`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. Ujistěte se, že je port volný.
`RESTAPI_Certificate`	Certifikát pro identifikaci požadavků (např. `RESTAPI_Certificate=C:\cert.pem`). Zabezpečená interakce aplikace Kaspersky Endpoint Security s klientem REST vyžaduje konfiguraci identifikace požadavku. K tomu musíte nainstalovat certifikát a následně podepsat payload každého požadavku.
`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.
`EnableUniqueSensorID`	Vytvoření jedinečného identifikátoru počítače (Sensor ID) během instalace nebo aktualizace aplikace. Sensor ID se v řešení Kaspersky Anti Targeted Attack Platform používá k identifikaci počítačů, které odesílají telemetrii na server. Při vytváření Sensor ID aplikace používá algoritmus, který bere v úvahu konfiguraci počítače, jako je například sériové číslo základní desky. V některých případech, například při používání aplikace ve virtuálním prostředí, může dojít k duplikaci Sensor ID. Kaspersky Anti Targeted Attack Platform tak nemůže identifikovat počítač, ze kterého je telemetrie odesílána. Chcete-li vytvořit jedinečné Sensor ID, musíte nastavit parametr `EnableUniqueSensorID=1`. Aplikace tak k vytvoření identifikátoru Sensor ID použije jiný algoritmus, který bere v úvahu jiná data o počítači. Tím je zajištěna jedinečnost Sensor ID. Ve výchozím nastavení není parametr nastaven. Aplikace zdědí Sensor ID v následujících případech: • aktualizace verze aplikace; • migrace konfigurace [KES+KEA] na konfiguraci [KES+integrovaný agent]. V rámci opravy aplikace se instalační program pokusí zdědit Sensor ID. Pokud Sensor ID nelze obnovit, aplikace vytvoří nový Sensor ID.
`SKIPKB5007186CHECK=1`	Zakázání kontroly nainstalované aktualizace operačního systému KB5007186. Před instalací aplikace instalační program zkontroluje nainstalované aktualizace operačního systému. Aktualizace KB5007186 je na seznamu aktualizací operačního systému, které mohou pro aplikaci působit problémy. Podrobné informace naleznete ve znalostní bázi technické podpory. Instalační služba proto v případě objevení této aktualizace přeruší instalaci. Chcete-li pokračovat v instalaci, nastavte `SKIPKB5007186CHECK=1`.

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.

  Chcete-li použít nastavení ze souboru setup.ini, umístěte tento soubor do složky, která obsahuje distribuční balíček aplikace Kaspersky Endpoint Security.

- install.cfg – nastavení činnosti aplikace Kaspersky Endpoint Security

  Pokud chcete používat nastavení z konfiguračního souboru install.cfg, musíte zadat cestu k souboru v následujícím příkazu při instalaci aplikace: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – klíč 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 souboru setup.reg, umístěte tento soubor 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=<path to the setup.reg file>`.

Setup /x. Odebrání aplikace

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 instalace v bezobslužném režimu nemusíte během instalace provádět žádnou činnost (bezobslužná odinstalace). 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 ve znalostní bázi technické podpory nebo pomocí následujícího příkazu:

     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   - Pokud je proces odebrání chráněn heslem:

     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x

     nebo

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

Můžete také použít parametr `SAVEQB` k ukládání souborů zkontrolovaných aplikací a umístěných do zálohy. Záložní kopie souborů jsou uloženy ve složce `C:\ProgramData\Kaspersky Lab\KES.14.0\QB`. Ve výchozím nastavení je ukládání souborů do zálohy zakázáno (`SAVEQB=0`).

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

msiexec /i. Obnovení aplikace

Při obnovování aplikace zkontroluje a obnoví integritu všech poškozených modulů aplikace a klíčů systémového registru vytvořených v rámci procesu instalace aplikace.

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

- V interaktivním režimu za použití průvodce instalací aplikace.
- V bezobslužném režimu. Po spuštění obnovení v bezobslužném režimu nemusíte během obnovování provádět žádnou činnost.

Pokud je instalační program aplikace Kaspersky Endpoint Security spuštěn v režimu obnovení a aplikace nepotřebuje obnovení, instalační program neprovede žádné změny.

Pokud je instalační program aplikace Kaspersky Endpoint Security spuštěn v režimu obnovení a aplikace není nainstalována, instalační program zahájí proces instalace.

Obnovení 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 obnovení není chráněn heslem:

     msiexec.exe /i <GUID> REINSTALL=ALL /qn

     `<GUID>` je jedinečný identifikátor aplikace. GUID aplikace můžete zjistit ve znalostní bázi technické podpory nebo pomocí následujícího příkazu:

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

   - Pokud je proces obnovení chráněn heslem:

     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn

`Příklad`

msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn

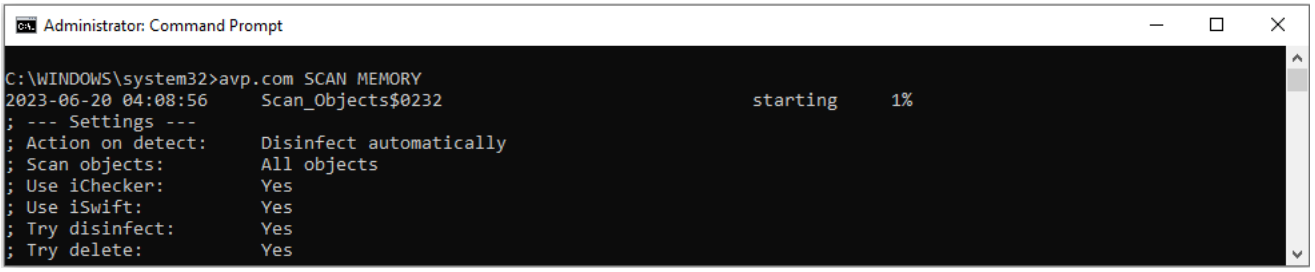
Příkazy AVP

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.
   Cestu ke spustitelnému souboru můžete přidat do systémové proměnné %PATH% během instalace aplikace.
3. K provedení příkazu použijte následující šablonu:

   avp.com <command> [options]

Výsledkem je, že Kaspersky Endpoint Security provede příkaz (viz obrázek níže).



Správa aplikace z příkazového řádku

SCAN. Kontrola malwaru

Spuštění úlohy *Kontrola malwaru*.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]

Rozsah kontroly

`<files to scan>` — 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 *Kontrola malwaru*. Aplikace Kaspersky Endpoint Security kontroluje tyto objekty:

- Paměť jádra;
- objekty načítané při spouštění operačního systému;
- Spouštěcí sektory;
- záloha operačního systému;

- Všechny pevné disky a vyměnitelné jednotky.

> V aplikaci Kaspersky Endpoint Security pro systém Windows 12.12 je z rozsahu kontroly aplikace vyloučen e-mail. Kontrolu příchozích a odchozích e-mailových zpráv provádí součást Ochrana před hrozbami v poště. Pokud používáte dřívější verzi modulu plug-in pro správu, aplikace vyloučí z rozsahu kontroly e-maily, i když je zásady zahrnují.

`/MEMORY`	Kontrola paměti jádra
`/STARTUP`	Kontrola objektů načítaných při spouštění operačního systému
`/REMDRIVES`	Zkontroluje vyměnitelné jednotky.
`/FIXDRIVES`	Zkontroluje pevné disky.
`/NETDRIVES`	Zkontroluje síťové jednotky.
`/QUARANTINE`	Zkontroluje soubory v záloze aplikace Kaspersky Endpoint Security.
`/@:<file list.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 informovat**. 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 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 se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor odstraní. Tato akce je nastavena jako výchozí.
`/i3`	**Odstranit, pokud se dezinfekce nezdaří**. Odstraní také složené soubory (například archivy), pokud infikovaný soubor nelze dezinfikovat nebo odstranit.
`/i4`	**Odstranit**. Odstraní také složené soubory (například archivy), pokud infikovaný soubor nelze odstranit.

Typy souborů

`/fe`	**Soubory kontrolované podle přípony**. Je-li toto nastavení povoleno, aplikace zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.
`/fi`	**Soubory kontrolované podle formátu**. Je-li toto nastavení povoleno, aplikace 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 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:<file mask>`	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:<seconds>`	Z rozsahu kontroly jsou vyloučeny soubory, jejichž kontrola trvá déle, než je zadaný časový limit (v sekundách).
`-es:<megabytes>`	Z rozsahu kontroly jsou vyloučeny soubory, které jsou větší než zadaný limit velikosti (v megabajtech).

Ukládání událostí do režimu souboru zprávy (pouze u profilů Kontrola, Aktualizace a Vrácení změn)

`/R:<report file>`	Uloží do souboru zprávy pouze kritické události.
`/RA:<report file>`	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:<file with scan settings>`	Soubor s nastavením úlohy *Kontrola malwaru*. Soubor musí být vytvořen ručně a uložen ve formátu TXT. Soubor může mít následující obsah: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

`Příklad`

avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"

UPDATE. Aktualizace databází a softwarových modulů aplikace

Spuštění úlohy *Aktualizace databází a modulů aplikace*.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

> Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

`Syntaxe příkazu`

avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]

Aktualizace nastavení úlohy

`local`	Spuštění úlohy *Aktualizace databází a modulů aplikace*, která byla vytvořena automaticky po instalaci aplikace. Nastavení úlohy *Aktualizace databází a modulů aplikace* 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 databází a modulů aplikace* s výchozím nastavením nebo s nastavením uvedeným v příkazu. Nastavení úlohy *Aktualizace databází a modulů aplikace* můžete nakonfigurovat následujícím způsobem: • `UPDATE` spustí úlohu *Aktualizace databází a modulů aplikace* s výchozím nastavením: zdroj aktualizací jsou servery aktualizace společnosti Kaspersky, účet je System a použijí se další výchozí nastavení. • `UPDATE local` spustí úlohu *Aktualizace databází a modulů aplikace*, která byla automaticky vytvořena po instalaci (předdefinovaná úloha). • `UPDATE <update settings>` spustí úlohu *Aktualizace databází a modulů aplikace* s ručně definovaným nastavením (viz níže).

Aktualizační zdroj

`"<update source>"`	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 zprávy (pouze u profilů Kontrola, Aktualizace a Vrácení změn)

`/R:<report file>`	Uloží do souboru zprávy pouze kritické události.

`/RA:<report file>`	Uloží do souboru zprávy všechny události.

Rozšířené nastavení

`/C:<file with update settings>`	Soubor s nastavením úlohy *Aktualizace databází a modulů aplikace*. Soubor musí být vytvořen ručně a uložen ve formátu TXT. Soubor může mít následující obsah: `["<update source>"] [/R[A]:<report file>]`.

`Příklad`
avp.com UPDATE local

avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt

ROLLBACK. Vrácení změn provedených poslední aktualizací

Vrácení poslední aktualizace 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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

> Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

`Syntaxe příkazu`
avp.com ROLLBACK [/R[A]:<report file>]

Ukládání událostí do režimu souboru zprávy (pouze u profilů Kontrola, Aktualizace a Vrácení změn)

`/R:<report file>`	Uloží do souboru zprávy pouze kritické události.
`/RA:<report file>`	Uloží do souboru zprávy všechny události.

`Příklad`
avp.com ROLLBACK /RA:rollback.txt

TRACES. 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.14.0\Traces`. Ve výchozím nastavení je trasování zakázáno.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`
avp.com TRACES on|off [<tracing level>] [<advanced settings>]

Úroveň trasování

`<tracing level>`	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 `file` a `mem`.
`file`	Uloží jeden soubor trasování (bez omezení velikosti).

`rot`	Uloží trasování do omezeného počtu sad souborů s omezenou velikostí; když je dosaženo maximální velikosti, přepíše starší soubory.
`mem`	Uloží trasování do souborů výpisu.

```
Příklad
```
avp.com TRACES on 500

avp.com TRACES off

avp.com TRACES on 500 mem

avp.com TRACES off file

START. Spuštění profilu

Spuštění profilu (například spuštění aktualizace databáze nebo povolení součásti ochrany).

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com START <profile> [/R[A]:<report file>]
```

Profil

`<profile>`	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 zprávy (pouze u profilů Kontrola, Aktualizace a Vrácení změn)

`/R:<report file>`	Uloží do souboru zprávy pouze kritické události.
`/RA:<report file>`	Uloží do souboru zprávy všechny události.

```
Příklad
```
avp.com START Scan_Objects

STOP. Zastavení profilu

Zastavení provádění profilu (například 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**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil

`<profile>`	Název profilu. *Profil* je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Seznam dostupných profilů můžete zobrazit příkazem `HELP STOP`.

Ověření

`/login=<user name> /password=<password>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

STATUS. Stav profilu

Zobrazení informací o stavu u profilů aplikací (například `running` nebo `completed`). 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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com STATUS [<profile>]
```

Pokud příkaz zadáte bez profilu, aplikace Kaspersky Endpoint Security zobrazí stav u všech profilů aplikace.

STATISTICS. Statistiky provozu profilu

Zobrazení statistiky u profilu aplikace (například doba trvání kontroly nebo počet zjištěných hrozeb). Seznam dostupných profilů můžete zobrazit příkazem `HELP STATISTICS`.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com STATISTICS <profile>
```

RESTORE. Obnovení souborů ze zálohy

Obovení souboru ze zálohy do jeho původní složky. Pokud v zadané cestě už existuje soubor se stejným názvem, aplikace požádá o potvrzení nahrazení souboru. 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.14.0\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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Rozšířené nastavení

`/REPLACE`	Přepíše existující soubor.
`<file name>`	Název souboru, který má být obnoven.

Ověření

`/login=<user name> /password=<password>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

```
Příklad
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Export nastavení aplikace

Export nastavení aplikace Kaspersky Endpoint Security do souboru. Pokud příkaz obsahuje pouze název souboru, do kterého chcete exportovat nastavení, aplikace umístí soubor následovně:

- Pokud je cesta k avp.com přidána do systémové proměnné %PATH%, aplikace umístí soubor do složky `C:\Windows\SysWOW64`.
- Pokud příkaz spustíte z instalační složky aplikace, export se nezdaří, protože vlastní ochrana aplikace blokuje vytvoření nového souboru ve složce aplikace. Chcete-li exportovat nastavení aplikace do souboru, zadejte cestu k souboru.

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Export nastavení**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>

Profil

`<profile>` Název profilu. *Profil* je součást, úloha nebo funkce aplikace Kaspersky Endpoint Security. Seznam dostupných profilů můžete zobrazit příkazem `HELP EXPORT`.

Soubor k exportu

`<file name>` Název souboru, do kterého se exportuje nastavení aplikace. Cestu k souboru můžete rovněž zadat ručně. Nastavení aplikace Kaspersky Endpoint Security můžete exportovat do konfiguračního souboru DAT nebo CFG, textového souboru TXT nebo dokumentu XML.

Ověření

`/login=<user name> /password=<password>` Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

`Příklad`

avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat

avp.com EXPORT fm fm_config.txt

IMPORT. Import nastavení aplikace

Import 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**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com IMPORT <file name> /login=<user name> /password=<password>

Soubor k importu

`<file name>` 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.

Ověření

`/login=<user name> /password=<password>` Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

`Příklad`

avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword

ADDKEY. Použití souboru klíče

Aktivace aplikace Kaspersky Endpoint Security pomocí aktivačního kódu. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

`Syntaxe příkazu`

avp.com ADDKEY <file name> [/login=<user name> /password=<password>]

Soubor klíče

`<file name>`	Název souboru klíče.

Ověření

`/login=<user name> /password= <password>`	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

Správa licenčních klíčů pro Kaspersky Endpoint Security, EDR Optimum nebo EDR Expert (doplněk Kaspersky Endpoint Detection and Response).

Chcete-li provést tento příkaz a odstranit licenční klíč, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Odstranit klíč**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

Syntaxe příkazu

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Operace

`/ADD <file name>`	Aktivace aplikace Kaspersky Endpoint Security pomocí aktivačního kódu. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.
`/ADD <activation code>`	Aktivuje aplikaci Kaspersky Endpoint Security pomocí aktivačního kódu. Pokud je aplikace již aktivována, bude klíč přidán jako rezervní.
`/REFRESH`	Aktualizace stavu licence k aplikaci Kaspersky Endpoint Security. Aplikace tak získá aktuální informace o stavu licence z aktivačních serverů společnosti Kaspersky.
`/REFRESH <license ID>`	Aktualizace stavu licencí pomocí ID licence. Pomocí tohoto příkazu můžete aktualizovat stav doplňku EDR, doplňku MDR, doplňku KUMA nebo jiných licencí. ID licence můžete získat z licenčního certifikátu. Aplikace tak získá aktuální informace o stavu licence z aktivačních serverů společnosti Kaspersky.
`/CHECK`	Načtení informací o licenci. Kaspersky Endpoint Security zobrazuje informace o všech přidaných licenčních klíčích včetně rezervních klíčů, doplňku EDR, doplňku MDR, klíčů doplňku KUMA a dalších klíčů. Kaspersky Endpoint Security zobrazuje následující informace o licenci: • název licence; • identifikátor licence; • adresa serveru pro ochranu (SVM), ke kterému je připojen virtuální počítač, na kterém je aplikace nainstalovaná, v režimu Light Agent; • typ licence: zkušební, komerční, beta, předplatné; • datum a čas aktivace aplikace; • datum a čas vypršení platnosti licence; • počet dní do vypršení platnosti licence.
`/CHECK <license ID>`	Načtení informací o licenci podle ID. Tento příkaz můžete použít k načtení informací o licenci. ID licence můžete získat z licenčního certifikátu.
`/DEL /login=<user name> /password=<password>`	Odebrání licenčního klíče k aplikaci. Bude odstraněn i rezervní klíč.
`/DEL <license ID> /login= <user name> /password= <password>`	Odstranění klíče pomocí ID licence. Pomocí tohoto příkazu můžete odstranit klíč z doplňku EDR, doplňku MDR, doplňku KUMA nebo jiných licencí. ID licence můžete získat z licenčního certifikátu.

Ověření

`/login=<user name> /password=<password>`	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 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Příklad
avp.com LICENSE /ADD file.key

avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD

avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword

RENEW. Zakoupení licence

Otevření webu Kaspersky, kde si můžete zakoupit nebo obnovit licenci.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

EXIT. Ukončení aplikace

Ukončení aplikace 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**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Syntaxe příkazu

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. 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**.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Syntaxe příkazu

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Povolení zásad

Povolení zásady sady softwaru Kaspersky Security Center v počítači. Nastavení aplikací bude nakonfigurováno podle těchto zásad.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

DISABLE. Zakázání ochrany

Zakázání součásti Ochrana před souborovými hrozbami 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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

SPYWARE. Detekce spywaru

Správa detekce spywaru. Detekce spywaru je ve výchozím nastavení povolena.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
avp.com SPYWARE on|off
```

KSN. Přepínání mezi KSN/KPSN

Výběr řešení Kaspersky pro určení reputace souborů nebo webových stránek. Kaspersky Endpoint Security podporuje následující infrastrukturní řešení pro práci s databázemi reputace Kaspersky:

- *Kaspersky Security Network (KSN)* je řešení, které používá většina aplikací Kaspersky. Účastníci služby KSN získávají od společnosti Kaspersky informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází reputace a statistik.
- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

```
Syntaxe příkazu
avp.com KSN /global | /private <file name>
```

Konfigurační soubor Kaspersky Security Network	
`<file name>`	Název konfiguračního souboru obsahujícího nastavení služby Kaspersky Private Security Network. Tento soubor má příponu PKCS7 nebo PEM.

Příklad

```
avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7
```

```
Příklad
avp.com KSN /global

avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Zákaz ochrany připojení k serveru

Spuštění úlohy *Ochrana připojení k serveru pro správu*, která odebere heslo počítače pro připojení k serveru pro správu. Úloha tak zakáže ochranu připojení k serveru pro správu.

Chcete-li provést tento příkaz, musí být povolena ochrana heslem.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```
avp.com SERVERBINDINGDISABLE [/password=<password>]

Heslo

`/password=<password>` — Heslo k uživatelskému účtu KL Admin nebo heslo z úlohy *Ochrana připojení k serveru pro správu*.

Pokud není tento parametr zadán, aplikace Kaspersky Endpoint Security vás na dalším řádku vyzve k zadání hesla.

Příkazy KESCLI

Příkazy KESCLI vám umožňují získávat informace o stavu počítačové ochrany pomocí součásti OPSWAT a umožňuje vám provádět standardní úlohy, jako jsou *Kontrola malwaru* a *Aktualizace databází a modulů aplikace*.

Seznam příkazů KESCLI zobrazíte příkazem `kescli --help` nebo zkráceným příkazem `kescli -h`.

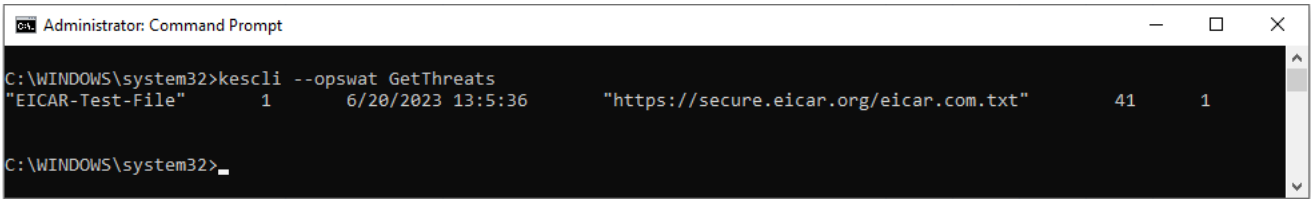
Postup správy aplikace Kaspersky Endpoint Security z příkazového řádku:

1. Spusťte překladač příkazového řádku (cmd.exe) jako správce.
2. Přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

   Cestu ke spustitelnému souboru můžete přidat do systémové proměnné %PATH% během instalace aplikace.
3. K provedení příkazu použijte následující šablonu:

   kescli <příkaz> [options]

   Výsledkem je, že Kaspersky Endpoint Security provede příkaz (viz obrázek níže).



Správa aplikace z příkazového řádku

Scan. Kontrola malwaru

Spustí úlohu *Kontrola malwaru* (Úplná kontrola).

Pro spuštění úlohy musí správce v zásadě povolit použití místních úloh.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
```
kescli --opswat Scan "<scan scope>" <action on threat detection>

Stav úlohy *Kontrola malwaru* můžete zjistit příkazem `GetScanState` a datum a čas posledního dokončení kontroly příkazem `GetLastScanTime`.

Rozsah kontroly

`<scan scope>` — Seznam souborů a složek oddělených `;`. Například `"C:\Program Files (x86)\Example Folder"`.

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 se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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

Zobrazení informací o stavu provádění úlohy *Kontrola malwaru* (*Úplná kontrola*):

- `1` – kontrola probíhá.
- `0` – kontrola není spuštěna.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

Syntaxe příkazu

```
kescli --opswat GetScanState
```

GetLastScanTime. Stanovení času dokončení kontroly

Zobrazení informací o datu a času posledního dokončení úlohy *Kontrola malwaru* (*Úplná kontrola*).

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

Syntaxe příkazu

```
kescli --opswat GetLastScanTime
```

GetThreats. Získání údajů o zjištěných hrozbách

Zobrazení seznamu zjištěných hrozeb (*Report on threats*). Tato zpráva obsahuje informace o hrozbách a aktivitě virů za posledních 30 dní před vytvořením zprávy.

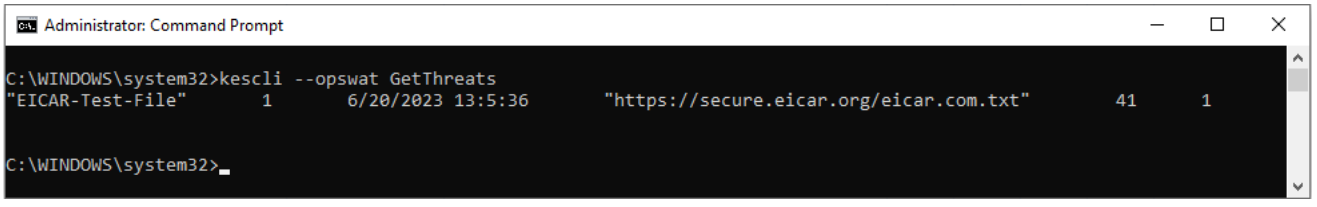
Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

Syntaxe příkazu

```
kescli --opswat GetThreats
```

Je-li proveden tento příkaz, aplikace Kaspersky Endpoint Security odešle odpověď v následujícím formátu:

```
<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection>
<threat danger level>
```



Správa aplikace z příkazového řádku

Typ objektu

0	Neznámý (`Unknown`).
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 (`Packed`).
20	Neznámé objekty (`Xfiles`).

21	Známé aplikace (`Software`).
22	Skryté soubory (`Hidden`).
23	Aplikace vyžadující pozornost (`Pupware`).
24	Anomální chování (`Anomaly`).
30	Nezjištěno (`Undetect`).
40	Reklamní bannery (`Banner`).
50	Síťový útok (`Attack`).
51	Přístup k registru (`Registry`).
52	Podezřelá aktivita (`Suspicion`).
60	Slabá místa (`Vulnerability`).
70	Phishing (`Phishing`).
80	Nechtěná e-mailová příloha (`Attachment`).
90	Malware zjištěný službou Kaspersky Security Network (`Urgent`).
100	Neznámý odkaz (`Suspic URL`).
110	Jiný malware (`Behavioral`).

Akce při zjištění hrozby

0	Neznámý (`unknown`).
1	Hrozba byla napravena (`ok`).
2	Objekt byl infikován a nebyl dezinfikován (`infected`).
5	Objekt je v archivu a nebyl dezinfikován (`archive`).
9	Objekt byl dezinfikován (`disinfected`).
10	Objekt nebyl dezinfikován (`not disinfected`).
11	Objekt byl odstraněn (`deleted`).
13	Byla vytvořena záložní kopie objektu (`backupped`).
15	Objekt byl přesunut do zálohy (`quarantined`).
23	Objekt byl odstraněn při restartu počítače (`delete on reboot`).
25	Objekt byl dezinfikován při restartu počítače (`disinfect on reboot`).
29	Objekt byl přesunut do zálohy uživatelem (`added by user`).
30	Objekt byl přidán k výjimkám (`added to exclude`).
31	Objekt byl přesunut do zálohy při restartu počítače (`quarantine on reboot`).
36	Falešně pozitivní výsledek (`false alarm`).
38	Proces byl ukončen (`terminated`).
40	Objekt nebyl zjištěn (`not found`).
41	Hrozbu nelze vyřešit (`untreatable`).
42	Objekt byl obnoven (`rolled back`).
43	Objekt byl vytvořen jako výsledek aktivity hrozby (`produced by threat`).
44	Objekt byl obnoven při restartu počítače (`roll back on reboot`).
0xffffffff	Objekt nebyl zpracován (`discarded`).

Úroveň rizika hrozby

`0`	Neznámá
`1`	Vysoká

2	Střední kontrola
4	Nízká
8	Informační (nižší než *Nízká*)

UpdateDefinitions. Aktualizace databází a softwarových modulů aplikace

Spuštění úlohy *Aktualizace databází a modulů aplikace*. Aplikace Kaspersky Endpoint Security používá výchozí zdroj: aktualizační servery Kaspersky.

> Pro spuštění úlohy musí správce v zásadě povolit použití místních úloh.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

> Tento příkaz nelze spustit, pokud je aplikace nainstalována v režimu Light Agent.

```
Syntaxe příkazu
kescli --opswat UpdateDefinitions
```

Datum a čas vydání aktuální virové databáze můžete zobrazit příkazem `GetDefinitionsetState`.

GetDefinitionState. Určení data a času poslední aktualizace databází

Zobrazení informací o datu a čase poslední aktualizace používaných antivirových databází.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
kescli --opswat GetDefinitionState
```

EnableRTP. Povolování ochrany

Povolení součásti ochrany aplikace Kaspersky Endpoint Security v počítači: Ochrana před souborovými hrozbami, Ochrana před webovými hrozbami, Ochrana před hrozbami v poště, Ochrana před síťovými hrozbami, Prevence narušení hostitele.

> Aby bylo možné povolit součásti ochrany, musí se správce ujistit, že lze upravit příslušná nastavení zásad (atributy jsou otevřené).

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
kescli --opswat EnableRTP
```

V důsledku toho jsou součásti ochrany povoleny, i když jste zakázali úpravy nastavení aplikace pomocí funkce Ochrana heslem.

Provozní stav součásti Ochrana před souborovými hrozbami můžete zkontrolovat příkazem `GetRealTimeProtectionState`.

GetRealTimeProtectionState. Stav součásti Ochrana před souborovými hrozbami

Zobrazení informací o stavu součásti Ochrana před souborovými hrozbami:

- `1` – součást je povolena.
- `0` – součást je zakázána.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Stav šifrování disku

Zobrazení informací o stavu šifrování disku:

- `1` znamená, že je disk chráněn produktem Kaspersky nebo technologií šifrování disku BitLocker.
- `0` znamená, že disk není šifrován.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
kescli --opswat GetEncryptionState
```

Version. Určení verze aplikace

Zobrazení verze aplikace Kaspersky Endpoint Security pro systém Windows.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security.

```
Syntaxe příkazu
kescli --Version
```

Můžete rovněž použít zkrácený příkaz `-v`.

Příkazy pro součást Detection and Response

Pomocí příkazového řádku můžete spravovat integrované funkce řešení Detection and Response (například Kaspersky Sandbox nebo Kaspersky Endpoint Detection and Response Optimum). Pokud není možná správa pomocí konzoly aplikace Kaspersky Security Center, můžete spravovat řešení Detection and Response. Seznam příkazů pro správu aplikace můžete zobrazit provedení příkazu `HELP`. Chcete-li si přečíst syntaxi konkrétního příkazu, zadejte `HELP <command>`.

Chcete-li spravovat integrované funkce řešení Detection and Response pomocí 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. K provedení příkazu použijte následující šablonu:

   ```
   avp.com <command> [options]
   ```

   Výsledkem je, že Kaspersky Endpoint Security provede příkaz.

SANDBOX. Správa součásti Sandbox

Příkazy pro správu součásti Sandbox:

- Povolení nebo zakázání součásti Sandbox.

  Součásti Sandbox poskytují interakci s řešením Kaspersky Sandbox a součástí KATA Sandbox, která je součástí řešení Kaspersky Anti Targeted Attack Platform.

- Konfigurace součásti Kaspersky Sandbox:

  - Připojení počítače k serverům Sandbox.

    Servery používají ke spouštění objektů, které je třeba kontrolovat nasazené bitové kopie operačních systémů Microsoft Windows. Můžete zadat IP adresu (IPv4 nebo IPv6) nebo plně kvalifikovaný název domény. Podrobnosti o nasazení virtuálních bitových kopií a konfiguraci serverů Sandbox naleznete v nápovědě k součásti Kaspersky Sandbox a nápovědě k řešení Kaspersky Anti Targeted Attack Platform.

  - Konfigurace časového limitu připojení pro server.

    Vypršel časový limit připojení pro Sandbox (u Kaspersky Sandbox) nebo server Central Node (u KATA). Po uplynutí nastaveného časového limitu odešle aplikace Kaspersky Endpoint Security požadavek na další server. Pokud je rychlost připojení nízká nebo je připojení nestabilní, můžete prodloužit časový limit připojení pro server. Doporučovaný časový limit požadavku je 0,5 sekundy a méně.

  - Konfigurace důvěryhodného připojení mezi počítačem a servery.

    Chcete-li nakonfigurovat důvěryhodné připojení se serverem Sandbox (u Kaspersky Sandbox) nebo serverem Central Node (u KATA), musíte si připravit certifikát TLS. Poté musíte přidat certifikát do počítače pomocí zásady. Certifikát musíte také přidat na server Sandbox (u Kaspersky Sandbox) nebo na server Central Node (u KATA).

  - Konfigurace režimu integrace.

    Je třeba vybrat řešení, jehož součástí je Sandbox, to znamená Kaspersky Sandbox nebo KATA Sandbox. *Kaspersky Sandbox* je samostatné řešení Detection and Response od společnosti Kaspersky. *KATA Sandbox* je součástí řešení Kaspersky Anti Targeted Attack Platform. Po integraci s KATA Sandbox může součást fungovat v následujících režimech:

    - **Manually**. Uživatel ručně odešle soubor ke kontrole z kontextové nabídky (**Odesílat do řešení Sandbox**).
    - **Automatically**. Aplikace automaticky detekuje objekty a odesílá je do součásti Sandbox ke kontrole.
    - **Combined**.

- Zobrazení aktuálního nastavení součásti.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Syntaxe příkazu

avp.com stop sandbox [/login=<user name> /password=<password>]

avp.com start sandbox

avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]

Operace

`stop` Zakázání součásti Sandbox.

`start` Povolení součásti Sandbox.

`set` Konfigurace součásti Sandbox. Nakonfigurovat můžete následující nastavení:

- Přidání serverů Sandbox (`--servers`)
- Přidání certifikátu TLS (`--pinned-certificate`)
- Přidání kryptokontejneru (`--client-certificate`)
- Zadejte heslo pro kryptokontejner (`--client-certificate-password`);
- Nastavení časového limitu připojení serveru (`--timeout`)
- Vyberte režim integrace (`--mode`:):
  - `KSB` – integrace s řešením Kaspersky Sandbox;
  - `KATAManual` – ruční integrace s KATA Sandbox;
  - `KATAAuto` – automatická integrace s KATA Sandbox;
  - `KATAFull` – kombinovaná integrace s KATA Sandbox.

`show` Zobrazit aktuální nastavení součásti. Zobrazí se následující odpověď:

```
sandbox.timeout=<Sandbox server connection timeout (ms)>
sandbox.servers=<list of Sandbox servers>
sanbox.mode=<integration mode>
sandbox.tls=<trusted connection status>
```

Ověření

`/login=<user name> /password=<password>` Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad

avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password

PREVENTION. Správa Prevence spouštění

Zakázání součásti Prevence spouštění nebo zobrazení aktuálního nastavení součásti, včetně seznamu pravidel prevence spouštění.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Syntaxe příkazu

avp.com prevention disable

avp.com prevention /show

Při provádění příkazu `prevention /show` dostanete následující odpověď:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
```

`sha256: <SHA256 hash of the file>`

`pattern: <path to the object>`

`case-sensitive: true|false`

Návratové hodnoty příkazů:

- `-1` znamená, že příkaz není podporován verzí aplikace, která je v počítači nainstalována.
- `0` znamená, že příkaz byl úspěšně proveden.
- `1` znamená, že příkazu nebyl předán povinný argument.
- `2` znamená, že došlo k obecné chybě.
- `4` znamená, že došlo k chybě syntaxe.
- `9` – nesprávná operace (například pokus o deaktivaci součásti, pokud je již deaktivována).

ISOLATION. Správa izolace sítě

Zakázání izolace počítače v síti nebo zobrazení aktuálního nastavení součásti. Nastavení součástí zahrnuje také seznam síťových připojení přidaných do výjimek.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com isolation /OFF /login=<user name> /password=<password>

avp.com isolation /STAT

V důsledku spuštění příkazu `stat` obdržíte následující odpověď: `Network isolation on|off`.

RESTORE. Obnovení souborů z karantény

Obovení souboru z karantény do jeho původní složky. *Karanténa* je speciální místní úložiště v počítači. Uživatel může umístit do karantény soubory, které považuje za nebezpečné pro počítač. Soubory v karanténě jsou uloženy v šifrovaném stavu a neohrožují zabezpečení zařízení. Aplikace Kaspersky Endpoint Security použije karanténu, pouze je-li integrována s řešeními Kaspersky Detection and Response. V ostatních případech aplikace Kaspersky Endpoint Security umístí příslušný soubor do zálohy. Podrobnosti o správě karantény jako součásti řešení najdete v nápovědě k řešení Kaspersky Sandbox, nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum, nápovědě k řešení Kaspersky Endpoint Detection and Response Expert, nápovědě k řešení Kaspersky Anti Targeted Attack Platform a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise).

Chcete-li provést tento příkaz, musí být povolena ochrana heslem. Uživatel musí mít oprávnění **Obnovit ze zálohy**.

Objekt je umístěn do karantény pod systémovým účtem (SYSTEM).

Obnova souborů z karantény zahrnuje následující zvláštní aspekty:

- Pokud byla cílová složka odstraněna nebo uživatel nemá k této složce přístupová práva, aplikace umístí soubor do složky `%DataRoot%\QB\Restored`. Poté musíte soubor ručně přesunout do cílové složky.
- Aplikace u názvu obnovovaného souboru rozlišuje malá a velká písmena. Pokud při zadávání názvu souboru nedbáte na velikost písmen, aplikace soubor neobnoví.
- Pokud cílová složka již obsahuje soubor se stejným názvem, aplikace obnovu souboru zruší.
- Pokud používáte řešení KATA (EDR), aplikace po obnovení souboru uloží kopii souboru do karantény. Karanténu můžete vyprazdňovat ručně. U řešení EDR Optimum a EDR Expert aplikace po obnovení soubor odstraní.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>

Rozšířené nastavení

`/REPLACE`	Přepíše existující soubor.

`<file name>` Název souboru, který má být obnoven.

Ověření

`/login=<user name> /password=<password>` Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

Příklad

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Návratové hodnoty příkazů:

- `-1` znamená, že příkaz není podporován verzí aplikace, která je v počítači nainstalována.
- `0` znamená, že příkaz byl úspěšně proveden.
- `1` znamená, že příkazu nebyl předán povinný argument.
- `2` znamená, že došlo k obecné chybě.
- `4` znamená, že došlo k chybě syntaxe.

IOCSCAN. Vyhledávání indikátorů narušení (IOC)

Spuštění úlohy *IOC Scan. Indikátor narušení (IOC)* je sada dat o objektu nebo činnosti, která indikuje neoprávněný přístup k počítači (narušení dat). Indikátor narušení může například představovat mnoho neúspěšných pokusů o přihlášení do systému. Úloha *IOC Scan* umožňuje v počítači najít tyto indikátory narušení a přijmout opatření jako reakci na hrozby.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

Kontrola IOC je přerušena po 128 shodách s indikátory narušení popsanými v pravidlech IOC. Je to nutné k omezení počtu položek ve zprávě o kontrole IOC, aby se usnadnila analýza a aby byla zpráva chráněna před přetečením z důvodu nepřesně formulovaných indikátorů narušení, což může generovat velké množství shod.

Syntaxe příkazu

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

Soubory IOC

`<full path to the IOC file>` Úplná cesta k souboru IOC, který chcete použít pro kontrolu. Můžete zadat více souborů IOC oddělených mezerami. Úplnou cestu k souboru IOC je nutné zadat bez argumentu `/path`.

Například `C:\Users\Admin\Desktop\IOC\file1.ioc`

`/path=<path to the folder with IOC files>` Cesta ke složce se soubory IOC, které chcete použít pro kontrolu. *Soubory IOC* jsou soubory obsahující sady indikátorů, které se aplikace pokusí porovnat, aby započítala detekci. Soubory IOC musí odpovídat standardu OpenIOC.

Například `C:\Users\Admin\Desktop\IOC`

Datový typ pro kontrolu IOC

`/process=on|off` Při provádění kontroly IOC (výraz ProcessItem) analyzujte data procesů.

Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security při provádění kontroly neanalyzuje procesy spuštěné v počítači. Pokud soubor IOC obsahuje výrazy IOC dokumentu ProcessItem IOC, jsou ignorovány (je zjištěno, že se neshodují).

Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data procesů, pouze pokud je dokument ProcessItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.

`/hint=<full path to the executable file of the process|full path to the file>` Při provádění kontroly IOC (výrazy ProcessItem a FileItem) analyzujte data souborů.

Soubor lze vybrat jedním z následujících způsobů:

- `<full path to the executable file of the process>` – výraz ProcessItem;
- `<full path to the file>` – výraz FileItem.

`/registry=on|off` Při kontrole IOC (výraz RegistryItem) analyzujte data registru Windows.

	Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje registr Windows. Pokud soubor IOC obsahuje výrazy dokumentu RegistryItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje registr Windows, pouze pokud je dokument RegistryItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu. U datového typu RegistryItem aplikace Kaspersky Endpoint Security kontroluje sadu klíčů registru.
`/dnsentry=on|off`	Při kontrole IOC (výraz DnsEntryItem) analyzujte data o záznamech v místní mezipaměti DNS. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje místní mezipaměť DNS. Pokud soubor IOC obsahuje výrazy dokumentu DnsEntryItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje místní mezipaměť DNS, pouze pokud je dokument DnsEntryItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/arpentry=on|off`	Při provádění kontroly IOC (výraz ArpEntryItem) analyzujte data o záznamech v tabulce ARP. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje tabulku ARP. Pokud soubor IOC obsahuje výrazy dokumentu ArpEntryItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje tabulku ARP, pouze pokud je dokument ArpEntryItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/ports=on|off`	Analyzujte data o portech otevřených k příjmu dat při provádění kontroly IOC (výraz PortItem). Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje tabulku aktivních připojení a zařízení. Pokud soubor IOC obsahuje výrazy dokumentu PortItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje tabulku aktivních připojení, pouze pokud je dokument PortItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/services=on|off`	Analyzujte data o službách nainstalovaných na zařízení při provádění kontroly IOC (výraz ServiceItem). Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje data o službách nainstalovaných na zařízení. Pokud soubor IOC obsahuje výrazy dokumentu ServiceItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data služeb, pouze pokud je dokument ServiceItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/system=on|off`	Při provádění kontroly IOC (výraz SystemInfoItem) analyzujte data prostředí. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje data prostředí. Pokud soubor IOC obsahuje výrazy dokumentu SystemInfoItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data prostředí, pouze pokud je dokument SystemInfoItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/users=on|off`	Při provádění kontroly IOC (výraz UserItem) analyzujte data o uživatelích. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje data o uživatelích vytvořených v systému. Pokud soubor IOC obsahuje výrazy dokumentu UserItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data o uživatelích vytvořených v systému, pouze pokud je dokument UserItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/volumes=on|off`	Při provádění kontroly IOC (výraz VolumeItem) analyzujte data o svazcích. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje data o svazcích na zařízení. Pokud soubor IOC obsahuje výrazy dokumentu VolumeItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data o svazcích, pouze pokud je dokument VolumeItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/eventlog=on|off`	Při kontrole IOC (výraz EventLogItem) analyzujte data o záznamech v protokolu událostí systému Windows.

	Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje záznamy v protokolu událostí systému Windows. Pokud soubor IOC obsahuje výrazy dokumentu EventLogItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje protokol událostí systému Windows, pouze pokud je dokument EventLogItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/datetime=<event publication date>`	Při určování rozsahu kontroly IOC pro příslušný dokument IOC vezměte v úvahu datum, kdy byla událost publikována v protokolu událostí systému Windows. Při provádění kontroly aplikace Kaspersky Endpoint Security kontroluje položky protokolu událostí systému Windows publikované v období od zadaného času a data do okamžiku spuštění úlohy. Kaspersky Endpoint Security umožňuje zadat jako hodnotu argumentu datum publikace události. Kontrola se provádí pouze u událostí publikovaných v protokolu událostí systému Windows po zadaném datu a před spuštěním kontroly. Není-li argument zadán, Kaspersky Endpoint Security kontroluje události s libovolným datem zveřejnění. Nastavení `TaskSettings::BaseSettings::EventLogItem::datetime` nelze upravit. Toto nastavení se použije pouze v případě, že je dokument EventLogItem IOC popsán v souboru IOC poskytnutém pro kontrolu.
`/channel=<list of channels>`	Seznam názvů kanálů (protokolů), pro které chcete provést kontrolu IOC. Pokud je zadán argument, aplikace Kaspersky Endpoint Security kontroluje záznamy publikované v zadaných protokolech. Dokument IOC musí mít popsaný výraz EventLogItem. Název protokolu je uveden jako řetězec v souladu s názvem protokolu (kanálu) uvedeným ve vlastnostech protokolu (parametr Full Name) nebo ve vlastnostech události (parametr `<Channel>` `</Channel>` ve schématu xml události). Můžete zadat více kanálů oddělených mezerami. Není-li argument zadán, aplikace Kaspersky Endpoint Security kontroluje záznamy pro kanály `Application`, `System`, `Security`.
`/files=on|off`	Při provádění kontroly IOC (výraz FileItem) analyzujte data souboru. Pokud je hodnota argumentu `off`, Kaspersky Endpoint Security nekontroluje data souborů. Pokud soubor IOC obsahuje výrazy dokumentu FileItem IOC, jsou ignorovány (zjištěno, že se neshodují). Není-li argument zadán, aplikace Kaspersky Endpoint Security analyzuje data souborů, pouze pokud je dokument FileItem IOC popsán v souboru IOC, který je poskytnut pro kontrolu.
`/drives=` `<all|system|critical|custom>`	Nastavte rozsah kontroly IOC při analýze dat pro dokument FileItem IOC. Pro rozsah kontroly můžete nastavit následující hodnoty: • `<all>` pro všechny dostupné rozsahy souborů. • `<system>` pro soubory ve složkách, kde je nainstalován operační systém. • `<critical>` pro dočasné soubory v uživatelských a systémových složkách. • `<custom>` pro soubory v uživatelsky definovaných oborech (`/scope=<list of folders to scan>`). Pokud argument není zadán, kontrola se provede pro kritické oblasti.
`/excludes=<list of exclusions>`	Nastavte rozsah výjimek při analýze dat pro dokument FileItem IOC. Můžete zadat více cest oddělených mezerami.
`/scope=<list of folders to scan>`	Uživatelem definovaný rozsah kontroly IOC při analýze dat pro dokument FileItem IOC (`/drives=custom`). Můžete zadat více cest oddělených mezerami.
`/retro /<number of days>`	*Retrospektivní kontrola IOC* je režim úlohy *IOC Scan*, ve kterém aplikace Kaspersky Endpoint Security kontroluje indikátory narušení pomocí dat za určité časové období. Tento režim je určen pro hledání indikátorů narušení podle telemetrie chráněného počítače, jako je síťová aktivita, procesy, soubory a jiná telemetrie. Můžete nastavit časové období od 1 do 14 dní. Ve výchozím nastavení aplikace vyhledává indikátory narušení bezpečnosti pro jeden den.
`/network=on|off`	Analýza síťových dat (výraz NetworkItem).
`/url=on|off`	Analýza dat v protokolech prohlížeče (výraz UrlHistoryItem). Retrospektivní kontrola IOC analyzuje protokoly následujících prohlížečů: Google Chrome, Mozilla Firefox, Microsoft Edge (verze 79 nebo novější).
`/email`	Analýza objektů pošty (výraz EmailItem).
`/route`	Analýza tabulek směrování a přesměrování (výraz RouteEntryItem).

Návratové hodnoty příkazů:

- `-1` znamená, že příkaz není podporován verzí aplikace, která je v počítači nainstalována.

- `0` znamená, že příkaz byl úspěšně proveden.
- `1` znamená, že příkazu nebyl předán povinný argument.
- `2` znamená, že došlo k obecné chybě.
- `4` znamená, že došlo k chybě syntaxe.

Pokud byl příkaz úspěšně proveden (návratová hodnota `0`) a přitom byly detekovány indikátory narušení, aplikace Kaspersky Endpoint Security odesílá na příkazový řádek následující informace o výsledku úlohy:

`Uuid`	ID souboru IOC ze záhlaví struktury souboru IOC (značka `<ioc id="">`)
`Name`	Popis souboru IOC ze záhlaví struktury souboru IOC (značka `<description></description>`)
`Matched Indicator Items`	Seznam ID všech odpovídajících indikátorů.
`Matched objects`	Data pro každý dokument IOC, pro který byla shoda.

MDRLICENSE. Aktivace MDR

Přidání konfiguračního souboru k aktivaci řešení 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 nápovědě 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 ( ).

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

`Syntaxe příkazu`

avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]

Operace

`/ADD <file name>`	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.

Ověření

`/login=<user name> /password=<password>`	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=samplePassword
```

`Příklad`

avp.com MDRLICENSE /ADD file.key

avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword

EDRKATA. Integrace s EDR (KATA)

Příkazy pro správu řešení Endpoint Detection and Response (KATA):

- Povolení nebo zakázání součásti EDR (KATA).
  Součást EDR (KATA) poskytuje interoperabilitu s řešením Kaspersky Anti Targeted Attack Platform.
- Konfigurace připojení k serverům platformy Kaspersky Anti Targeted Attack Platform.
- Zobrazení aktuálního nastavení součásti.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```

avp.com START EDRKATA

avp.com STOP EDRKATA

avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]

avp.com edrkata /show

Operace	
`stop`	Zakázání součásti EDR (KATA).
`start`	Povolení součásti EDR (KATA).
`set`	Konfigurace součásti EDR (KATA). Nakonfigurovat můžete následující nastavení: • Přidání serverů součásti Central Node (`servers=<server address>:<port>`) • Přidání certifikátu TLS (`server-certificate=<path to the TLS certificate>`) • Nastavení časového limitu připojení serveru Central Node (`/timeout=<Central Node server connection timeout (s)>`) • Nastavení období pro synchronizaci se serverem Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	Zobrazit aktuální nastavení součásti.

KUMA. Integrace s KUMA

Příkazy pro správu integrovaného agenta KUMA:

- Povolení nebo zakázání integrace KUMA.

  Integrovaný agent KUMA poskytuje interoperabilitu s řešením Kaspersky Unified Monitoring and Analysis Platform.
- Probíhá konfigurace připojení k serverům Kaspersky Unified Monitoring and Analysis Platform.
- Zobrazení aktuálního nastavení součásti.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```

avp.com START KUMA

avp.com STOP KUMA [/login=<user name> /password=<password>]

avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [/client-certificate-password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]

avp.com KUMA /SHOW

Operace	
`stop`	Zakázání integrace KUMA.
`start`	Povolení integrace KUMA.
`set`	Konfigurace integrovaného agenta KUMA. Nakonfigurovat můžete následující nastavení: • Přidání serverů KUMA (`/servers=<protocol>://<server address>:<port>`) Aplikace podporuje následující protokoly připojení k serveru: `tcp`, `udp`, `http`, `https`. • Přidání certifikátu TLS (`/server-certificate=<path to the TLS certificate>`) • Nastavení časového limitu připojení serveru (`/timeout=<KUMA server connection timeout (s)>`) • Přidání kryptokontejneru (`/client-certificate=<path to the crypto-container> /client-certificate-password=<password>`) • Konfigurace prodlevy přenosu událostí (`/maximum-data-transfer-time=<maximum events transmission delay (sec)>`)

`show`	Zobrazit aktuální nastavení součásti.

Ověření

`/login=<user name> /password=<password>`	Přihlašovací údaje k uživatelskému účtu s požadovanými oprávněními k ochraně heslem.

```
Příklad
```
avp.com start kuma

avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15 /login=login /password=password

avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer /login=login /password=password

YARA. Spuštění kontroly YARA

Spuštění úlohy *Spustit kontrolu YARA*. Aplikace kontroluje soubory a objekty, zda neobsahují indikátory cílených útoků na podnikovou IT infrastrukturu pomocí databází pravidel YARA. *Pravidla YARA* jsou popisy signatur cílených útoků a narušení podnikové infrastruktury IT, které Kaspersky Endpoint Security používá ke kontrole objektů.

Chcete-li spustit kontrolu YARA, musíte připravit soubory YARA, které popisují pravidla. Při vytváření souborů YARA zvažte následující požadavky:

- Kaspersky Endpoint Security podporuje soubory YARA s příponou .YARA nebo .YAR, které dodržují otevřený standard YARA 4.2.3 pro popis indikátorů narušení.
- Pro úlohu lze zadat pouze soubory s pravidly YARA. Úloha *Spustit kontrolu YARA* nepodporuje jiné typy pravidel.
- Pokud jste přidali soubory YARA, které Kaspersky Endpoint Security nepodporuje, nebo pokud pravidla obsahují chyby syntaxe, úloha bude přerušena s příslušnou chybovou zprávou.
- Identifikátory všech souborů YARA používaných v jedné úloze musí být jedinečné. Pokud neexistují žádné soubory YARA se stejným identifikátorem, může to mít vliv na výsledky provádění úlohy.
- Kontrola YARA je přerušena po 128 shodách s indikátory popsanými v pravidlech YARA. Je to nutné k omezení počtu položek ve zprávě o kontrole YARA, aby se usnadnila analýza a aby byla zpráva chráněna před přetečením z důvodu nepřesně formulovaných pravidel YARA, což může generovat velké množství shod.

Kaspersky doporučuje vytvořit jedno pravidlo pro každý soubor YARA. Výsledky kontroly jsou tak čitelnější.

Kontrola YARA může trvat značně dlouho. V závislosti na velikosti jednotky, nastavení úlohy a počtu objektů na disku může kontrola YARA trvat od několika minut až po několik hodin. Aplikace nezobrazuje indikátor průběhu. Zastavit ani zrušit kontrolu YARA nelze. Doporučujeme vám počkat, až budou k dispozici její výsledky.

```
Syntaxe příkazu
```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]

Soubory YARA

`<full path to the YARA file>`	Úplná cesta k souboru YARA, který chcete použít pro kontrolu. Můžete zadat cesty k více souborům YARA odděleným mezerami. Povinný argument, pokud není zadána hodnota `/path=<path to the folder with YARA files>`. Příklad: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`
`/path=<path to the folder with YARA files>`	Úplná cesta ke složce se soubory YARA, které chcete použít pro kontrolu. Povinný argument, pokud není zadána hodnota `<full path to the YARA file>`. Příklad: `/path=C:\Users\Admin\Desktop\YARA`

Rozšířené nastavení

`/fastScan=<on|off>`	Rychlá kontrola YARA. U každého objektu aplikace protokoluje jeden výskyt zjištěného indikátoru. Aplikace také v protokolu skryje duplikáty zjištěných indikátorů. Rychlá kontrola YARA umožňuje rychlejší kontrolu velkých souborů. Není-li toto nastavení zadáno, aplikace provede standardní kontrolu YARA. V tomto režimu aplikace protokoluje duplikáty zjištěných indikátorů.
`/maxRules=<maximum number of scan rules>`	Limit počtu jedinečných aktivovaných pravidel, při jehož dosažení aplikace zastaví kontrolu YARA.

	Pokud není zadaná hodnota tohoto nastavení nebo pokud je zadána hodnota `0`, aplikace provede kontrolu YARA bez omezení.
`/timeOut=<stop scan after the specified time in seconds>`	Jak dlouho může kontrola YARA trvat (v sekundách). Po uplynutí této doby aplikace zastaví kontrolu YARA. Pokud není zadaná hodnota tohoto nastavení nebo pokud je zadána hodnota `0`, aplikace provede kontrolu YARA bez omezení.
`/recursive=<on|off>`	Tento argument spouští rekurzivní kontrolu podsložek v rámci vlastní kontroly `/scanFolders`.
`/scanFolders=<list of folders to be scanned>`	Tento argument spustí kontrolu souborů v zadaném seznamu složek YARA. Můžete zadat více hodnot oddělených mezerami. Při zadávání masky cesty ke složce podporuje aplikace Kaspersky Endpoint Security znaky `*` a `?`. Pokud toto nastavení není zadáno, aplikace provede kontrolu YARA všech místních disků kromě síťových sdílených položek, cloudových jednotek a vyměnitelných médií.
`/scanMemory=<on|off>`	Kontrola paměti všech spuštěných procesů.
`/scanProcess=<process name>`	Kontrola paměti pouze pro zadané procesy. Zadejte úplné cesty ke spustitelným souborům procesů oddělené mezerami. Můžete také zadat masku pomocí znaků `*` a `?`.
`/maxSize=<file size in bytes>`	Omezení velikosti souboru kontroly YARA. Aplikace přeskakuje větší soubory.
`/includes=<list of objects to be scanned>>`	Úprava rozsahu kontroly. Můžete zadat více hodnot oddělených mezerami. K dispozici jsou následující hodnoty: • Název souboru • Přípona souboru Rozsah kontroly je třeba specifikovat s parametrem `/scanFolders`. Příklad: `/scanFolders C:\*.* /includes=*.exe *.dll` – aplikace kontroluje všechny soubory s příponami EXE a DLL na disku C.
`/excludes=<list of objects to be scanned>`	Vyloučení souborů z kontroly YARA. Můžete zadat více hodnot oddělených mezerami. K dispozici jsou následující hodnoty: • Cesta k souboru • Maska cesty k souboru Výjimky je třeba specifikovat s parametrem `/scanFolders`. Příklad: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – aplikace přeskočí soubor readme.txt, všechny soubory ze složky C:\trusted a všechny soubory s příponou XML v kořenové složce na disku C.
`/scanAutoruns=<on|off>`	Kontrola YARA objektů bodu automatického spouštění.
`/excludeAutoruns=<list of autorun point areas to skip>`	Objekty bodu automatického spuštění jsou z rozsahu kontroly vyloučeny. Zadejte úplné cesty ke spustitelným souborům procesů oddělené mezerami. Můžete také zadat masku pomocí znaků `*` a `?`.
`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Pokud zadáte cestu ke složce, aplikace uloží výsledky kontroly v zadané cestě do souboru s názvem yara_<název počítače>_<čas dokončení kontroly>.txt. Pokud zadáte cestu ke konkrétnímu souboru TXT, aplikace uloží výsledky kontroly do tohoto souboru. Například: `/logFolder=C:\test` nebo `/logFolder=C:\test\abc.txt`. Výsledky kontroly jsou výstupem do příkazového řádku bez ohledu na to, zda je zadána možnost `/logFolder`.

Návratové hodnoty příkazů:

- `-1` znamená, že příkaz není podporován verzí aplikace, která je v počítači nainstalována.
- `0` znamená, že příkaz byl úspěšně proveden.
- `1` znamená, že příkazu nebyl předán povinný argument.
- `2` znamená, že došlo k obecné chybě.
- `4` znamená, že došlo k chybě syntaxe.
- `5` znamená, že nebyl nalezen jeden nebo více souborů s pravidly YARA zadanými v parametru.

Pokud byl příkaz úspěšně proveden (návratová hodnota `0`) a přitom byly detekovány indikátory narušení, aplikace Kaspersky Endpoint Security odesílá na příkazový řádek následující informace o výsledku úlohy:

`Started at <time>` `Finished at <time>`	Čas zahájení a čas dokončení kontroly.
`Host name: <computer name>`	Název počítače, na kterém byl objekt zjištěn.
`Result: <error>`	Kód chyby pro chybu, ke které došlo při provádění úlohy. Pokud se nevyskytnou žádné chyby, výstup aplikace je `0x00000000`.
`Comment: <comment text>`	Popis chyby pro chybu, ke které došlo při provádění úlohy. Například `Operation timeout`.
`Object Name:` nebo `Process:` (při kontrole paměti procesu)	Název objektu nebo procesu, u kterého bylo aktivováno pravidlo YARA.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hodnota hash objektu, u kterého bylo aktivováno pravidlo YARA.
`Rule Name`	Název aktivovaného pravidla YARA.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadata jsou určena v pravidlu YARA.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	V rámci objektu byly nalezeny shody, které splňují podmínky pravidla YARA:
	• Posun v paměti procesu nebo souboru, kde byla detekována shoda (`Offset`).
	• Název odpovídajícího řetězce v pravidle YARA (`String name`).
	• Odpovídající řetězec v paměti procesu nebo souboru (`String data`).

TELEMETRYFILTERS. Filtrování událostí, které mají být odeslány do sítě KUMA

Ve výchozím nastavení je odesílání událostí na server KUMA zakázáno. Aby server KUMA fungoval správně, musíte povolit odesílání telemetrie. Zdroj událostí můžete vybrat ze standardních protokolů: *Application*, *Security* nebo *System*. Chcete-li zvýšit výkon a optimalizovat přenos dat na server KUMA, můžete ručně přidat jednotlivé události nebo z ní vyloučit jednotlivé události. Můžete například vyloučit události sysmon.

Seznam výjimek můžete exportovat do souboru JSON z příkazového řádku.

Pokud příkaz obsahuje pouze název souboru, do kterého chcete exportovat nastavení, aplikace umístí soubor následovně:

- Pokud je cesta k avp.com přidána do systémové proměnné %PATH%, aplikace umístí soubor do složky `C:\Windows\SysWOW64`.
- Pokud příkaz spustíte z instalační složky aplikace, export se nezdaří, protože vlastní ochrana aplikace blokuje vytvoření nového souboru ve složce aplikace. Chcete-li exportovat nastavení aplikace do souboru, zadejte cestu k souboru.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```
avp.com TELEMETRYFILTERS /export <file name>

avp.com TELEMETRYFILTERS /import <file name>

Operace

`export`	Export filtrů událostí k odeslání do sítě KUMA.
`import`	Import filtrů událostí k odeslání do sítě KUMA. Pokud už v počítači existují pravidla filtrování událostí, aplikace Kaspersky Endpoint Security je při importu nahradí.

Soubor pro export nebo import

`<file name>`	Název souboru s filtry událostí, které mají být odeslány do sítě KUMA. Cestu k souboru můžete rovněž zadat ručně. Filtry pro odeslání do sítě KUMA můžete exportovat do souboru JSON.

Příkazy pro správu součásti Light Agent

Aplikaci můžete spravovat v režimu Light Agent za účelem ochrany virtuálních prostředí na příkazovém řádku. Pokud není možná správa pomocí konzoly aplikace Kaspersky Security Center, můžete spravovat aplikaci v režimu Light Agent. Seznam příkazů pro správu aplikace můžete zobrazit provedení příkazu `HELP`. Chcete-li si přečíst syntaxi konkrétního příkazu, zadejte `HELP <command>`.

Postup správy aplikace v režimu Light Agent 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. K provedení příkazu použijte následující šablonu:

   ```
   avp.com <command> [options]
   ```

   Výsledkem je, že Kaspersky Endpoint Security provede příkaz.

Aplikace nainstalovaná v režimu Light Agent podporuje téměř všechny příkazy AVP aplikace nainstalované ve standardním režimu. V režimu Light Agent jsou omezeny úlohy aktualizace antivirové databáze a úlohy správy licenčního klíče.

KSVLAINFO. Určení režimu součásti Light Agent

Určení režimu součásti Light Agent.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```
avp.com KSVLAINFO

Příkaz vypíše do konzoly následující informace:

- Režim Light Agent pro ochranu virtuálních prostředí: povolen nebo zakázán.

  Pokud je povolen režim Light Agent, aplikace se používá jako součást řešení Kaspersky Security for Virtualization Light Agent.

- Režim ochrany VDI: povolen nebo zakázán.

  Režim ochrany VDI pomáhá optimalizovat výkon aplikace Kaspersky Endpoint Security na neperzistentních virtuálních počítačích. Pokud je povolen režim ochrany VDI, aktualizace, které vyžadují restartování chráněného virtuálního počítače, se neinstalují na neperzistentní virtuální počítače. Při příjmu aktualizací, které vyžadují restartování, součást Light Agent nainstalovaná na neperzistentním virtuálním počítači odešle zprávu do aplikace Kaspersky Security Center, kde ji informuje, že šablonu chráněného virtuálního počítače je třeba aktualizovat.

- Typ chráněného virtuálního počítače: trvalý nebo neperzistentní.
- Role chráněného virtuálního počítače ve virtuální infrastruktuře: server nebo pracovní stanice.
- Identifikátor (UUID) chráněného virtuálního počítače.

VIISINFO. Stav připojení součásti Light Agent k integračnímu serveru

Zobrazení informací o připojení součásti Light Agent k integračnímu serveru.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```
avp.com VIISINFO

Příkaz vypíše do konzoly následující informace:

- Adresa a port integračního serveru, ke kterému je součást Light Agent připojena.
- Stav připojení k integračnímu serveru.
- Datum a čas posledního připojení součásti Light Agent k integračnímu serveru.

SVMINFO. Stav připojení součásti Light Agent k serveru pro ochranu

Zobrazení informací o připojení součásti Light Agent k serveru pro ochranu.

Pokud chcete příkaz spustit, přejděte do složky, ve které se nachází spustitelný soubor aplikace Kaspersky Endpoint Security. Můžete také přidat cestu ke spustitelnému souboru do systémové proměnné %PATH% a spustit příkaz bez přechodu do složky aplikace.

```
Syntaxe příkazu
```

avp.com SVMINFO

Příkaz vypíše do konzoly následující informace:

- Adresa serveru SVM, ke kterému je součást Light Agent připojena, a umístění SVM ve virtuální infrastruktuře vzhledem k součásti Light Agent: místní nebo nemístní.
- Způsob zjišťování SVM, který používá Light Agent: pomocí integračního serveru nebo vlastního seznamu adres SVM.
- Seznam adres SVM, pokud je jako metoda zjišťování SVM vybrán seznam adres SVM.
- Značka pro připojení součásti Light Agent k SVM.
- Algoritmus výběru SVM: standardní nebo rozšířený. Pokud se používá rozšířený algoritmus výběru SVM, zobrazuje se také typ cesty k SVM ve virtuální infrastruktuře.
- Stav ochrany připojení mezi součástí Light Agent a serverem pro ochranu.

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 `Error: Cannot start task 'EntAppControl'`. Aplikace Kaspersky Endpoint Security může také zobrazovat další informace ve formě kódu, například `error=8947906D` (viz tabulka níže).

Chybové kódy

Kód chyby	Popis
`09479001`	Tento klíč se již používá
`0947901D`	Platnost licence vypršela. Aktualizace databáze nejsou k dispozici
`89479002`	Klíč nenalezen
`89479003`	Digitální podpis chybí nebo je poškozen
`89479004`	Poškozená data
`89479005`	Poškozený soubor klíče
`89479006`	Platnost licence vypršela
`89479007`	Není určen soubor klíče
`89479008`	Neplatný soubor klíče
`89479009`	Uložení dat selhalo
`8947900A`	Čtení dat selhalo
`8947900B`	Chyba V/V
`8947900C`	Databáze nenalezeny
`8947900E`	Knihovna licencí nenačtena
`8947900F`	Databáze poškozeny nebo aktualizovány ručně
`89479010`	Databáze jsou poškozené
`89479011`	K přidání rezervního klíče nelze použít neplatný soubor klíče
`89479012`	Systémová chyba
`89479013`	Seznam zakázaných klíčů je poškozený
`89479014`	Podpis souboru se neshoduje s digitálním podpisem společnosti Kaspersky
`89479015`	Klíč pro zkušební licenci nelze použít jako klíč pro licenci komerční
`89479016`	K používání beta verze aplikace je nutná licence pro beta testování
`89479017`	Soubor klíče není kompatibilní s touto aplikací. Aplikaci Kaspersky Endpoint Security pro systém Windows nelze aktivovat pomocí souboru klíče pro jinou aplikaci. Zkontrolujte nainstalovanou aplikaci
`89479018`	Licenční klíč je blokován společností Kaspersky
`89479019`	Aplikace již byla použita se zkušební licencí. Klíč pro zkušební licenci nelze přidat znovu
`8947901A`	Poškozený soubor klíče

8947901B	Digitální podpis chybí, je poškozen nebo neodpovídá digitálnímu podpisu společnosti Kaspersky
8947901C	Klíč nelze přidat, pokud platnost příslušné nekomerční licence již vypršela
8947901E	Datum vytvoření nebo použití souboru klíče je neplatné. Zkontrolujte systémové datum
8947901F	Klíč pro zkušební licenci nelze přidat. Již je aktivní jiný klíč pro zkušební licenci
89479020	Seznam zakázaných klíčů je poškozený nebo chybí
89479021	Popis aktualizace chybí nebo je poškozený
89479022	Klíč nelze použít pro tuto aplikaci
89479023	K přidání rezervního klíče nelze použít neplatný soubor klíče
89479025	Chyba při odesílání žádosti na aktivační server. Možné důvody: Chyba připojení k internetu nebo dočasné problémy na aktivačním serveru. Zkuste aplikaci aktivovat později (za 1 až 2 hodiny) pomocí aktivačního kódu. Pokud chyba přetrvává, obraťte se na svého poskytovatele internetu
89479026	Žádost obsahuje nesprávný aktivační kód
89479027	Stav odpovědi nelze získat
89479028	Při ukládání dočasného souboru došlo k chybě
89479029	Je zadán nesprávný aktivační kód nebo je v počítači nastaveno neplatné systémové datum. Zkontrolujte systémové datum v počítači
8947902A	Klíč není s touto aplikací kompatibilní, nebo vypršela platnost licence
8947902B	Soubor klíče nebyl přijat. Byl zadán nesprávný aktivační kód
8947902C	Aktivační server vrátil chybu 400
8947902D	Aktivační server vrátil chybu 401
8947902E	Aktivační server vrátil chybu 403
8947902F	Potřebný prostředek aktivačního serveru je nedostupný. Aktivační server vrátil chybu 404. Zkontrolujte nastavení připojení k internetu
89479030	Aktivační server vrátil chybu 405
89479031	Aktivační server vrátil chybu 406
89479032	Je nutné ověření proxy serveru. Zkontrolujte nastavení sítě
89479033	Vypršel časový limit žádosti
89479034	Aktivační server vrátil chybu 409
89479035	Potřebný prostředek aktivačního serveru je nedostupný. Aktivační server vrátil chybu 410. Zkontrolujte nastavení připojení k internetu
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	Nepodporovaná funkce
8947903E	Neplatná odpověď brány. Zkontrolujte nastavení sítě
8947903F	Prostředek je dočasně nedostupný
89479040	Časový limit odpovědi brány vypršel. Zkontrolujte nastavení sítě
89479041	Server nepodporuje tento protokol
89479043	Neznámá chyba HTTP
89479044	Neplatné ID prostředku
89479046	Neplatná adresa URL
89479047	Neplatná cílová složka
89479048	Chyba přiřazení paměti

89479049	Při převodu parametrů do řetězce ANSI (adresa URL, složka, agent) došlo k chybě
8947904A	Při vytváření pracovního vlákna došlo k chybě
8947904B	Pracovní vlákno je již spuštěno
8947904C	Pracovní vlákno není spuštěno
8947904D	Soubor klíče nebyl na aktivačním serveru nalezen
8947904E	Klíč je zablokován
8947904F	Interní chyba aktivačního serveru
89479050	Nedostatek dat v žádosti o aktivaci
89479053	Platnost licence, která odpovídá přidanému klíči, již vypršela
89479054	V počítači je nastaveno neplatné systémové datum. Zkontrolujte hodnotu systémového data
89479055	Platnost zkušební licence vypršela
89479056	Lhůta pro aktivaci aplikace vypršela
89479057	Byl překročen limit aktivací aplikace pro zadaný kód
89479058	Proces aktivace byl dokončen se systémovou chybou
89479059	Klíč pro zkušební licenci nelze použít jako klíč pro licenci komerční
8947905C	Je vyžadován aktivační kód
89479062	Nelze se připojit k aktivačnímu serveru
89479064	Aktivační server je nedostupný. Zkontrolujte nastavení internetového připojení a zkuste aplikaci znovu aktivovat
89479065	Platnost licence vypršela
89479066	Aktivní klíč nelze nahradit klíčem, jehož platnost již vypršela
89479067	Nelze přidat rezervní klíč, pokud platnost příslušné licence vyprší před platností stávající licence
89479068	Chybí aktualizovaný klíč předplatného
8947906A	Neplatný aktivační kód
8947906B	Klíč je již aktivní
8947906C	Typy licencí odpovídajících aktivním a rezervním klíčům se neshodují
8947906D	Komponenta není licencí podporována
8947906E	Jako rezervní klíč nelze přidat klíč předplatného
89479213	Obecná chyba přenosné vrstvy
89479214	Nepodařilo se připojit k aktivačnímu serveru
89479215	Neplatný formát webové adresy
89479216	Adresu proxy serveru se nepodařilo převést
89479217	Převedení adresy serveru se nezdařilo. Zkontrolujte nastavení internetového připojení
89479218	Pokus o připojení k serveru selhal
89479219	Přístup byl vzdáleně odepřen
8947921A	Časový limit operace vypršel
8947921B	Chyba odesílání požadavku HTTP
8947921C	Chyba připojení SSL
8947921D	Operace přerušena zpětným voláním
8947921E	Příliš mnoho přesměrování
8947921F	Kontrola příjemce selhala
89479220	Prázdná odpověď ze serveru
89479221	Chyba odesílání dat

89479222	Chyba přijímání dat
89479223	Problém související s certifikátem SSL
89479224	Problém související s šifrováním SSL
89479225	Problém související s certifikačním centrem SSL
89479226	Neplatný obsah síťového paketu
89479227	Přístup k účtu byl odepřen
89479228	Neplatný soubor certifikátu SSL
89479229	Nelze uzavřít připojení SSL
8947922A	Opakující se chyba
8947922B	Neplatný soubor s odvolanými certifikáty
8947922C	Chyba požadavku certifikátu SSL
89479401	Neznámá chyba serveru
89479402	Interní chyba serveru
89479403	Pro zadaný aktivační kód není k dispozici žádný klíč
89479404	Aktivní klíč blokován
89479405	Chybí povinné parametry žádosti o aktivaci
89479406	Neplatné číslo nebo heslo klienta
89479407	Neplatný aktivační kód
89479408	Aktivační kód není kompatibilní s touto aplikací. Aplikaci Kaspersky Endpoint Security pro systém Windows nelze aktivovat pomocí aktivačního kódu pro jinou aplikaci. Zkontrolujte nainstalovanou aplikaci
89479409	Je vyžadován aktivační kód
8947940B	Aktivační doba vypršela
8947940C	Byl překročen počet aktivací pomocí tohoto kódu
8947940D	Neplatný formát ID žádosti
8947940E	Aktivační kód je již používán
8947940F	Aktivační kód se nepodařilo obnovit
89479410	Aktivační kód je neplatný pro tuto oblast
89479411	Pro lokalizaci této aplikace nelze tento aktivační kód použít
89479412	Aktivační kód je určen pro novou verzi této aplikace. Chcete-li aktivovat nainstalovanou verzi aplikace, pořiďte si jiný aktivační kód
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	Je vyžadován aktivační server verze 1.0
89479418	Nesprávný formát aktivačního kódu
89479419	Čas počítače není synchronní s časem aktivačního serveru
8947941A	Nesprávná verze aplikace
8947941B	Platnost předplatného vypršela
8947941C	Překročen počet aktivací
8947941D	Neplatný podpis tiketu
8947941E	Jsou potřeba další data
8947941F	Ověření dat selhalo
89479420	Neaktivní předplatné

89479421	Na aktivačním serveru probíhá údržba
89479501	Neočekávaná chyba
89479502	Přeneseny neplatné parametry. Například prázdný seznam adres aktivačního serveru
89479503	Neplatný aktivační kód (neplatná hodnota hash)
89479504	Neplatné ID uživatele
89479505	Neplatné heslo uživatele
89479506	Neplatná odpověď aktivačního serveru
89479507	Požadavek na aktivaci byl přerušen
89479509	Aktivační server vrátil prázdný seznam 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` a `EXPORT`. 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.
- `AntiCryptor`.
- `BehaviorDetection` – Detekce chování.
- `DeviceControl` – Kontrola zařízení.
- `EntAppControl` – Kontrola aplikací.
- `File_Monitoring` nebo `FM` – Ochrana před souborovými hrozbami.
- `Firewall` nebo `FW` – Brána firewall.
- `HIPS` – Prevence narušení hostitele.
- `IDS` – Ochrana před síťovými hrozbami.
- `IntegrityCheck` – Kontrola integrity.
- `LogInspector` – Kontrola protokolu.
- `Mail_Monitoring` nebo `EM` – Ochrana před hrozbami v poště.
- `Rollback` – Vrácení aktualizace (profil nelze použít, pokud je aplikace nainstalována v režimu Light Agent).
- `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 (profil nelze použít, pokud je aplikace nainstalována v režimu Light Agent).
- `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.

Příprava na instalaci aplikace s podporou REST API

Zabezpečená interakce aplikace Kaspersky Endpoint Security s klientem REST vyžaduje konfiguraci identifikace požadavku. K tomu musíte nainstalovat certifikát a následně podepsat payload každého požadavku.

K vytvoření certifikátu můžete použít např. OpenSSL.

Příklad:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Použijte šifrovací algoritmus RSA s délkou klíče 2048 bitů nebo více.

Získáte tak certifikát `cert.pem` certifikát a soukromý klíč `key.pem`.

Instalace aplikace pomocí rozhraní REST API

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=<user name>`

     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 správu aplikace prostřednictvím rozhraní REST API. Ve výchozím nastavení je použit port 6782. Ujistěte se, že je port volný. Volitelný parametr.

- `RESTAPI_Certificate=<path to certificate>`

  Certifikát pro identifikaci požadavků (např. `RESTAPI_Certificate=C:\cert.pem`).

  Certifikát můžete nainstalovat po instalaci aplikace nebo jej aktualizovat po vypršení platnosti certifikátu.

  Jak nainstalovat certifikát pro identifikaci požadavku API REST

  1. Zakázání sebeobrany aplikace Kaspersky Endpoint Security

     Mechanismus sebeobrany brání změnám či odstranění souborů aplikace na pevném disku, procesů v paměti a záznamů v systémovém registru.

  2. Přejděte na klíč registru, který obsahuje nastavení REST API:
     `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestApi`.

  3. Zadejte cestu k certifikátu, například `Certificate = C:\Folder\cert.pem`.

  4. Povolte sebeobranu aplikace Kaspersky Endpoint Security.

  5. Restartujte aplikaci.

- `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.

Příklad:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

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
```

Pokud jste nainstalovali aplikaci pomocí rozhraní REST API, aplikace Kaspersky Endpoint Security automaticky v nastavení součásti Kontrola webu vytvoří pravidlo povolení pro přístup k webovým prostředkům (*pravidlo služby pro REST API*). Toto pravidlo je nutné k tomu, aby měli klienti REST vždy přístup k aplikaci Kaspersky Endpoint Security. Pokud jste například omezili přístup uživatelů k webovým prostředkům, nebude to mít vliv na správu aplikace prostřednictvím rozhraní REST API. Doporučujeme, abyste toto pravidlo neodstraňovali ani neměnili nastavení *pravidla služby REST API*. Pokud jste pravidlo odstranili, aplikace Kaspersky Endpoint Security je obnoví po restartování aplikace.

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. Použijte strukturu nastavení přijatou v odpovědi na požadavek GET.

Příklad:

```
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. Uložte nastavení aplikace (payload) do formátu JSON (payload.json).

5. Podepište JSON ve formátu PKCS7.

Příklad:

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
signed_payload.pem
```

Získáte tak podepsaný soubor s payloadem požadavku (`signed_payload.pem`).

6. Upravte nastavení zásad. Chcete-li to provést, odešlete požadavek POST a připojte podepsaný soubor s payloadem požadavku (`signed_payload.pem`).

Aplikace použije nové nastavení a odešle odpověď obsahující výsledky konfigurace aplikace (odpověď může být prázdná). Aktualizaci nastavení můžete ověřit pomocí požadavku GET.

Zdroje informací o aplikaci

Tato část popisuje zdroje informací o aplikaci.

V závislosti na důležitosti a naléhavosti problému si můžete vybrat nejvhodnější zdroj informací.

Stránka aplikace Kaspersky Endpoint Security na webu společnosti Kaspersky

Na stránce aplikace Kaspersky Endpoint Security můžete zobrazit obecné informace o aplikaci a jejích funkcích a vlastnostech.

Stránka aplikace Kaspersky Endpoint Security obsahuje odkaz na online obchod. Tam si můžete aplikaci zakoupit nebo obnovit.

Stránka aplikace Kaspersky Endpoint Security ve znalostní bázi

Znalostní báze je sekce 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 často kladené otázky týkající se nákupu, instalace a používání aplikace.

Články znalostní báze mohou odpovědět na otázky týkající se nejen aplikace Kaspersky Endpoint Security, ale také dalších aplikací společnosti Kaspersky. Články ve znalostní bázi mohou obsahovat také novinky z technické podpory.

Diskuse o aplikacích společnosti Kaspersky na Fóru

Pokud vaše otázka nevyžaduje naléhavou odpověď, můžete o ní diskutovat s odborníky společnosti Kaspersky a dalšími uživateli na našem Fóru.

Na Fóru si můžete prohlížet existující témata, přidávat vlastní 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;
- konfigurací jednotlivých součástí aplikace změnou speciálních nastavení, která nejsou dostupná přes standardní uživatelské 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. Pokud nastavení aplikace sami změníte způsobem, který není popsán v online nápovědě nebo v doporučeních technické podpory, může to způsobit zpomalení a pády operačního systému, snížit úroveň ochrany počítače a poškodit dostupnost a integritu zpracovávaných informací.

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.14.0\Traces`.

Soubory trasování jsou pojmenovány takto: `KES<14.0_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.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.

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<14.0_dateXX.XX_timeXX.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 webová konzola aplikace Kaspersky Security Center, a to ve složce `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Soubory trasování webového modulu plug-in aplikace jsou pojmenovány následujícím způsobem: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.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 pro úlohu *Změna součástí 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 se ukládá do složky System Volume Information 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 provozu aplikace

Trasování aplikací jsou podrobné záznamy o akcích, které aplikace provedla, a o zprávách o událostech, ke kterým dochází během provozu aplikace. Během procesu trasování aplikace vytvoří sadu souborů s údaji o provozu různých součástí aplikace (například SRV.log, WD.log a další).

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 .
2. V okně, které se otevře, 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:
   - **S omezením velikosti**. Uloží trasování do omezeného počtu sad souborů s omezenou velikostí; když je dosaženo maximální velikosti, přepíše starší soubory. Pokud je vybrán tento režim, můžete definovat maximální počet sad souborů pro střídání a maximální velikost pro jednotlivé sady souborů.

Ve výchozím nastavení aplikace ukládá pět sad trasovacích souborů. Velikost jednotlivé sady souborů je 3072 MB. Pro uložení trasovacích souborů tak potřebujete 15 GB volného místa na disku.

- **Bez omezení**. Uloží jeden soubor trasování (bez omezení velikosti).

5. V rozevíracím seznamu **Úroveň** vyberte úroveň trasování:

   - **Normální** znamená, že soubor trasování ukládá zprávy o všech chybách, varování a také informace o běžném provozu aplikace (výchozí).
   - **Podrobně** znamená, že soubor trasování ukládá všechny informace o provozu aplikace.

   Další úrovně trasování jsou k dispozici, pokud spravujete nastavení trasování aplikace na příkazovém řádku. O požadované úrovni trasování se poraďte s odborníkem technické podpory. Pokud asistence technické podpory není k dispozici, nastavte úroveň trasování na možnost **Normální**.

   Pokud bylo na příkazovém řádku povoleno trasování aplikace a byla nastavena jiná úroveň trasování než **Normální** nebo **Podrobně**, **Úroveň** je rozevírací seznam nastaven na **Normální**.

6. Chcete-li zastavit proces trasování, vraťte se do okna **Podpůrné nástroje** a deaktivujte trasování.

Soubory trasování můžete také vytvořit při instalaci aplikace z příkazového řádku, včetně použití souboru setup.ini.

Soubory trasování provozu aplikace se tak vytvoří ve složce `%ProgramData%\Kaspersky Lab\KES.14.0\Traces`. Po vytvoření pošlete trasovací soubory technické podpoře společnosti Kaspersky.

Kaspersky Endpoint Security automaticky odstraní soubory trasování po odebrání aplikace. Soubory můžete rovněž odstranit ručně. To provedete tak, že musíte zakázat trasování a zastavit aplikaci.

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 .
2. V okně, které se otevře, 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:

   - **S omezením velikosti**. 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.
   - **Bez omezení**. Uloží jeden soubor trasování (bez omezení velikosti).

5. V rozevíracím seznamu **Úroveň** vyberte úroveň trasování:

   - **Základní**. Kaspersky Endpoint Security analyzuje nejdůležitější procesy operačního systému související s výkonem.
   - **Podrobně**. 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 Nástroje podpory a zakažte trasování.

   Soubor trasování výkonu se tak vytvoří ve složce `%ProgramData%\Kaspersky Lab\KES.14.0\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.14.0\Traces`.

Jak povolit zápis výpisu paměti v konzole pro správu (MMC)

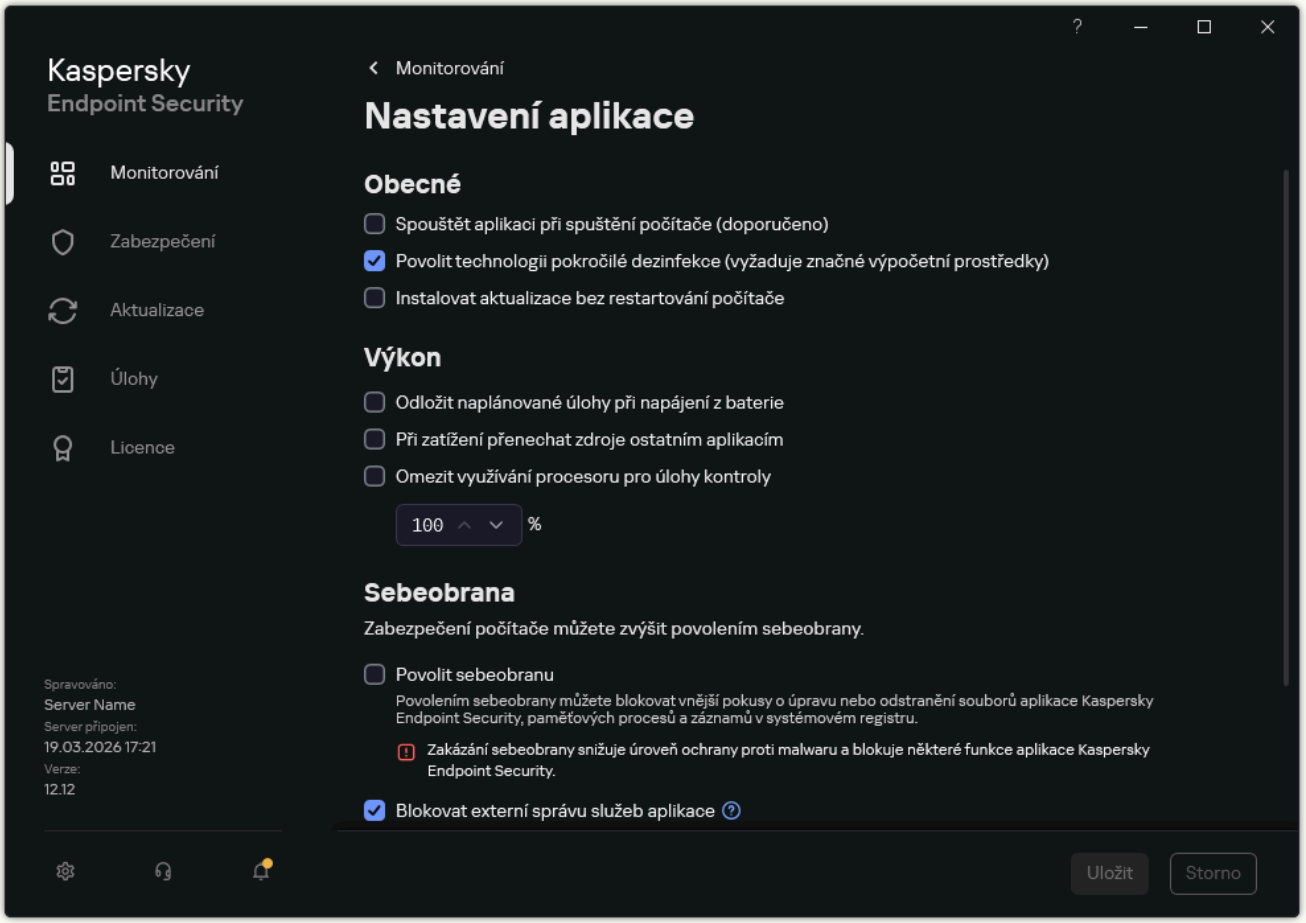
1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V bloku **Informace o ladění** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, pomocí zaškrtávacího políčka **Povolit zápis výpisu paměti** povolte nebo zakažte zápis výpisu paměti aplikace.
6. Uložte změny.

Jak povolit zápis výpisu paměti ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.
2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.
   Otevře se okno vlastností zásad.
3. Vyberte kartu **Application settings**.
4. Přejděte na **General Settings** → **Technical Support**.
5. V bloku **Debug information** pomocí zaškrtávacího políčka **Dump writing ENABLED** povolte nebo zakažte zápis výpisu paměti aplikace.
6. Uložte změny.

Jak povolit zápis výpisu paměti v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.
2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

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.

Jak povolit ochranu souborů výpisu a trasovacích souborů v konzole pro správu (MMC)

1. Ve stromu konzoly pro správu aplikace Kaspersky Security Center vyberte možnost **Policies**.
2. Vyberte potřebnou zásadu a dvojitým kliknutím otevřete vlastnosti zásady.
3. V okně zásad vyberte **Obecná nastavení** → **Nastavení aplikace**.
4. V bloku **Informace o ladění** klikněte na tlačítko **Nastavení**.
5. V okně, které se otevře, pomocí zaškrtávacího políčka **Povolit ochranu souborů výpisu a trasování** povolte nebo zakažte ochranu souborů.
6. Uložte změny.

Jak povolit ochranu souborů výpisu a trasovacích souborů ve webové konzole a cloudové konzole

1. V hlavním okně webové konzoly vyberte možnosti **Asset management** → **Policies**.

2. Klikněte na název zásad aplikace Kaspersky Endpoint Security.

   Otevře se okno vlastností zásad.

3. Vyberte kartu **Application settings**.

4. Přejděte na **General Settings** → **Technical Support**.

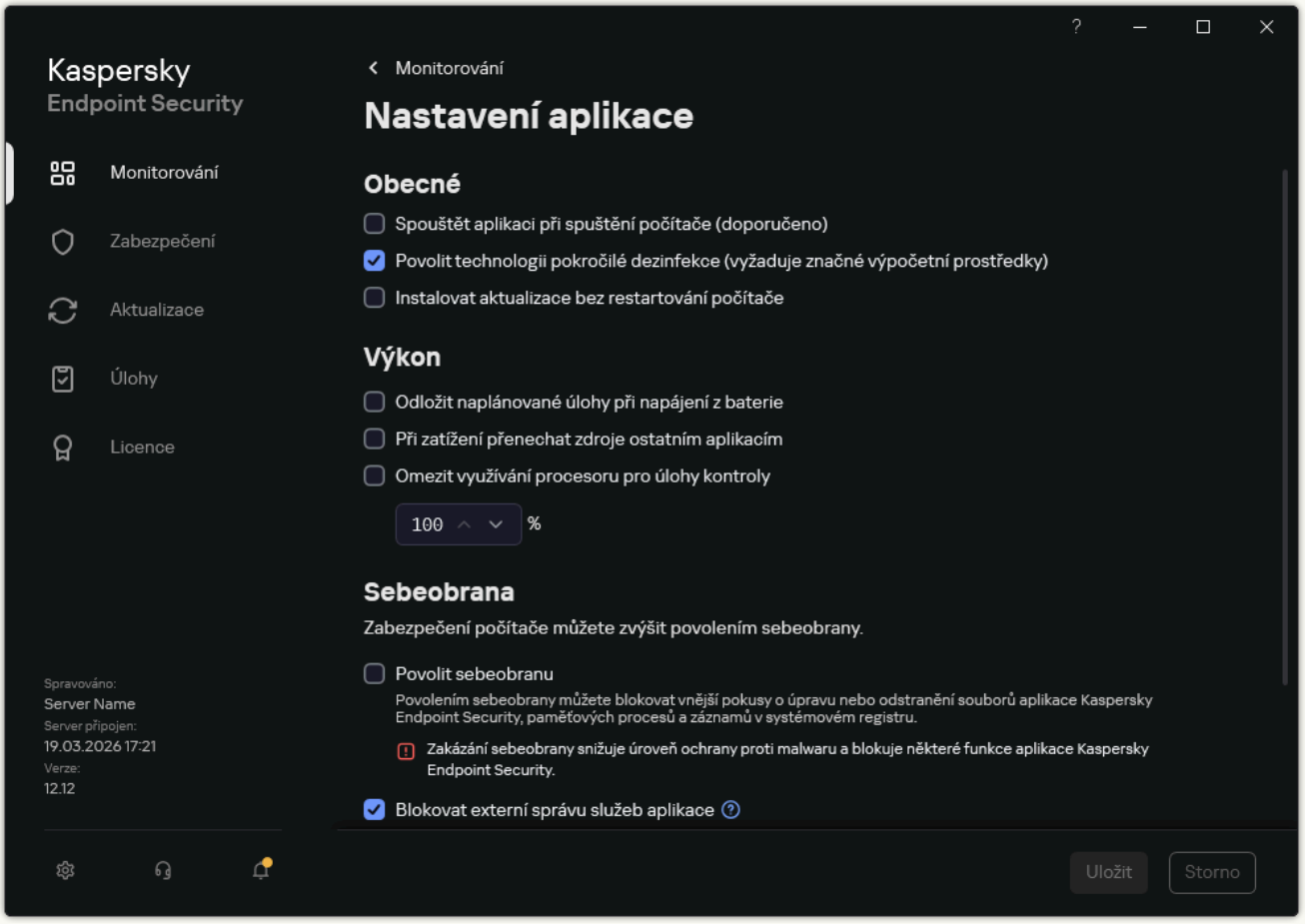
5. V bloku **Debug information** povolte nebo zakažte ochranu souborů pomocí zaškrtávacího políčka **Dump and trace files protection ENABLED**.

6. Uložte změny.

Jak povolit ochranu souborů výpisu a trasovacích souborů v rozhraní aplikace

1. V hlavním okně aplikace klikněte na tlačítko ⚙.

2. V okně nastavení aplikace vyberte možnost **Obecná nastavení** → **Nastavení aplikace**.



Nastavení aplikace Kaspersky Endpoint Security pro systém Windows

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.

Načítání dat operačního systému (Kaspersky Get System Info)

Po instalaci aplikace Kaspersky Endpoint Security nemusí operační systém nebo aplikace fungovat správně. Došlo ke konfliktu mezi aplikací a softwarem nebo ovladači součástí počítače.

Za účelem zjištění příčiny problému vyžaduje technická podpora společnosti Kaspersky zprávu od nástroje Kaspersky Get System Info (dále jen GSI). Podrobné informace o použití tohoto nástroje najdete ve znalostní bázi společnosti Kaspersky.

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.
- Podrobnosti o podpoře operačních systémů Microsoft Windows 11 a Microsoft Windows Server 2022 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 o 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.
- 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 debírání jednotlivých součástí aplikace (například pomocí úlohy *Změna součástí aplikace*) může být vyžadován restart počítače.
- Ve vlastnostech úlohy *Změna součástí aplikace* není podporována synchronizace kombinace součástí mezi jednotlivými režimy při změně režimu instalace (**Samostatný režim** / **Kombinovaný režim**). Kombinaci součástí mezi režimy aplikace synchronizuje poté, co znovu otevřete vlastnosti úlohy.
- 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.
- Pokud jste zrušili odebírání aplikace Kaspersky Endpoint Security, spusťte obnovení aplikace po restartování počítače.
- Aplikace vyžaduje Microsoft .NET Framework 4.0 nebo novější. Microsoft .NET Framework 4.6.1 má slabá místa. Pokud používáte Microsoft .NET Framework 4.6.1, musíte nainstalovat aktualizace zabezpečení. Podrobnosti o aktualizacích zabezpečení Microsoft .NET Framework najdete na webu technické podpory společnosti Microsoft.
- 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.
- 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.
- Při instalaci aplikace Kaspersky Endpoint Security pro systém Windows na server s nainstalovanými aplikacemi Kaspersky Security for Windows Server (KSWS) a Windows Defender je nutné systém restartovat. Restart systému je nutný i v případě, že jste povolili instalaci aplikace bez restartu systému. Windows Defender pro Windows Server je na seznamu softwaru, který je nekompatibilní s aplikací Kaspersky Endpoint Security pro systém Windows. Před instalací aplikace instalační program Windows Defender pro Windows Server odstraní. Odstranění nekompatibilního softwaru vyžaduje restart systému.
- Před instalací aplikace Kaspersky Endpoint Security pro systém Windows (KES) na server, kde je nainstalována aplikace Kaspersky Security for Windows Server (KSWS), musíte vypnout ochranu heslem KSWS. Po migraci z KSWS na KES povolte ochranu heslem v nastavení aplikace.
- Pro instalaci aplikace na počítače se systémy Windows 7 nebo Windows Server 2008 R2 s nasazeným softwarem Veeam Backup & Replication může být zapotřebí restartovat počítač a spustit aplikaci znovu.
- Migrace z aplikace Kaspersky Small Office Security (KSOS) na aplikaci Kaspersky Endpoint Security (KES) s povolenou součástí Ochrana heslem je k dispozici od KSOS sestavení 21.16.*.*. Pokud chcete provést migraci starších verzí KSOS, musíte součást Ochrana heslem zakázat nebo KSOS odebrat ručně. Migrace z KSOS na KES se zakázanou součástí Ochrana heslem se provádí správně.
- Kaspersky Endpoint Security nelze nainstalovat na spouštěcí vyměnitelnou jednotku. Při instalaci aplikace Kaspersky Endpoint Security zobrazí chybovou zprávu: *Vybrali jste neplatnou složku nebo jednotku. Aplikaci je nutné nainstalovat na místní pevný disk*. Pokud se vám aplikaci podaří nainstalovat na vyměnitelnou jednotku pomocí nástrojů třetích stran, může to způsobit selhání operačního systému (BSOD) během procesu zavádění. Znamená to, že aplikace Kaspersky Endpoint Security nepodporuje systém Windows To Go a podobná řešení. Ke kontrole počítače z vyměnitelné jednotky můžete použít bezplatnou aplikaci Kaspersky Rescue Disk.

- Při instalaci aplikace Kaspersky Endpoint Security se síťovými součástmi na terminálový server s víceuživatelskými relacemi RDP je potřeba brát v úvahu několik aspektů. Operační systémy vynutí ukončení všech uživatelských relací po skončení relace správce. Chcete-li se připojit k terminálovému serveru, musíte restartovat server nebo se přihlásit do systému místně. Toto chování je dáno fungováním operačního systému Windows.

- Pokud jsou v Kaspersky Security Center 16.0 nebo v Kaspersky Security Center 16.1 nainstalovány webové moduly plug-in aplikace Kaspersky Endpoint Security pro systém Windows (verze 12.11.0.2004) a Kaspersky Endpoint Security for Linux (verze 12.4.0.1354), aktualizace webového modulu plug-in aplikace Kaspersky Endpoint Security pro systém Windows na verzi 12.11.0.6004 může vést k poruchám v zásadách aplikace Kaspersky Endpoint Security for Linux.

  Možné řešení: přejděte do okna **Settings** → **Web plug-ins** a odeberete ze seznamu webový modul plug-in Kaspersky Endpoint Security pro systém Windows, webový modul plug-in Kaspersky Endpoint Security for Linux a Unified Protection and Management Plug-in. Poté nainstalujte nejprve webový modul plug-in aplikace Kaspersky Endpoint Security for Linux a poté webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows.

- Ve webové konzole se ve vlastnostech instalačního balíčku aplikace Kaspersky Endpoint Security 12.11 pro systém Windows nesprávně zobrazuje seznam součástí. Samostatná součást, Anti-Cryptor, není v této verzi aplikace k dispozici. Funkce ochrany sdílených složek před externím šifrováním je zahrnuta v součásti Detekce chování. V aplikaci Kaspersky Endpoint Security 12.12 pro systém Windows je tato funkce samostatnou součástí. Zároveň se v konzole pro správu (MMC) správně zobrazuje seznam součástí.

Upgrade aplikace

- 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 databází a modulů aplikace*, *Kontrola kritických oblastí*, *Vlastní kontrola* a *Kontrola integrity aplikací* neuloží.

- 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.

- Aplikace vyžaduje Microsoft .NET Framework 4.0 nebo novější. Microsoft .NET Framework 4.6.1 má slabá místa. Pokud používáte Microsoft .NET Framework 4.6.1, musíte nainstalovat aktualizace zabezpečení. Podrobnosti o aktualizacích zabezpečení Microsoft .NET Framework najdete na webu technické podpory společnosti Microsoft.

- Při upgradu aplikace Kaspersky Endpoint Security aplikace zakáže používání KSN, dokud není přijato Prohlášení o Kaspersky Security Network. Kromě toho lze stav počítače změnit v aplikaci Kaspersky Security Center na *Critical*: je přijata událost *Servery KSN nejsou k dispozici*. Pokud používáte řešení Kaspersky Managed Detection and Response, obdržíte události týkající se narušení provozu tohoto řešení. Pro provoz řešení Kaspersky Managed Detection and Response je nutné používání KSN. Kaspersky Endpoint Security umožňuje používání KSN po použití zásad, v nichž správce přijme podmínky používání KSN. Po přijetí Prohlášení o Kaspersky Security Network aplikace Kaspersky Endpoint Security bude opět fungovat.

- Po upgradu aplikace Kaspersky Endpoint Security na verzi 11.10.0 nebo novější bez restartu budou v počítači nainstalovány dvě aplikace Kaspersky Endpoint Security. Předchozí verzi aplikace neodstraňujte ručně. Předchozí verze se automaticky odstraní při restartování počítače.

- Po upgradu aplikace Kaspersky Endpoint Security v počítači se systémem Microsoft Windows 11 se v kontextové nabídce souboru mohou zobrazovat položky pro předchozí i novou verzi aplikace. Správnou funkci kontextové nabídky souboru zajistíte dvojím restartováním počítače.

- Pokud má aplikace vypnutou funkci Sebeobrana a všechny síťové adaptéry jsou zastavené, nebudou síťové součásti aplikace mezi ukončením upgradu aplikace a restartem počítače fungovat. Mezi síťové součásti aplikace patří Ochrana před webovými hrozbami, Ochrana před hrozbami v poště, Ochrana před síťovými hrozbami, Brána firewall, Prevence narušení hostitele a Kontrola webu. Pro správnou funkci aplikace restartujte počítač.

- Součást Ochrana před útoky BadUSB nefunguje mezi ukončením aktualizace aplikace a restartem počítače. Pro správnou funkci aplikace restartujte počítač.

- Aplikaci nelze upgradovat, pokud nebyl dokončen předchozí proces upgradu. Pro správnou funkci aplikace restartujte počítač.

- Po upgradu aplikace z verzí starších než Kaspersky Endpoint Security 11 pro Windows musí být počítač restartován.

- Pokud spravujete aplikaci Kaspersky Endpoint Security pomocí cloudové konzole aplikace Kaspersky Security Center, není místní aktualizace aplikace povolena. Při místní aktualizaci aplikace nelze přijmout smlouvu o zpracování dat pro cloudovou konzolu aplikace Kaspersky Security Center.

Podpora pro architekturu ARM

- Instalace aplikace Kaspersky Endpoint Security v režimu Light Agent na virtuálních počítačích s architekturou ARM není podporována.

- Technologie Kaspersky Disk Encryption není podporována na počítačích s architekturou ARM.
- Šifrování souborů není podporováno na počítačích s architekturou ARM.
- Šifrování vyměnitelných jednotek není podporováno na počítačích s architekturou ARM.
- V počítačích se systémem Windows 11 pro Arm64 není EDR Agent kompatibilní s Bitdefender Endpoint Security Tools.
- Funkce ochrany zvukového signálu a funkce ochrany přístupu k webové kameře nejsou podporovány na počítačích s architekturou ARM.
- V počítačích s architekturou ARM podporuje rozšíření Ochrana před hrozbami v poště 32bitové verze aplikace Outlook 2016, Outlook 2021, Outlook 2024 a Outlook 365 pro Arm64.
- Kaspersky Endpoint Security neodesílá objekty určené pro architekturu ARM do součásti Kaspersky Sandbox.
- Řízení tisku není podporováno na počítačích s architekturou ARM.
- Integrace s řešením Kaspersky Endpoint Detection and Response Expert (cloud) není podporována na počítačích s architekturou ARM.
- Na počítačích s architekturou ARM úloha *IOC Scan* podporuje e-mailové soubory pouze z následujících poštovních klientů: 32bitová a 64bitová verze aplikace Outlook 2016 a Outlook 2021, 2024 a 365 pro Arm64.

Podpora serverových platforem

- Na serverech s povolenou *deduplikací dat* musíte přidat soubor fsdmhost.exe na seznam důvěryhodných aplikací. Pomáhá to optimalizovat výkon aplikace a předcházet nadměrnému zatížení procesoru.
- Systém ReFS je podporován s určitými omezeními:
  - Aplikace Kaspersky Endpoint Security může nesprávně zpracovat události dezinfekce hrozeb. Pokud například aplikace odstranila škodlivý soubor, může mít zpráva položku Objekt nebyl zpracován. Aplikace Kaspersky Endpoint Security současně dezinfikuje hrozby v souladu s nastavením aplikace. Aplikace Kaspersky Endpoint Security může také vytvořit duplikát události *Objekt bude při restartu dezinfikován* pro stejný objekt.
  - Ochrana před souborovými hrozbami může některé hrozby přeskočit. Kontrola malwaru přitom funguje správně.
  - Po spuštění úlohy *Kontrola malwaru* jsou výjimky přidané pomocí nástroje iChecker resetovány při restartu serveru.
  - Technologie iSwift není podporována. Kaspersky Endpoint Security nebere v úvahu výjimky z kontroly přidané pomocí technologie iSwift.
  - Pokud byl před instalací aplikace Kaspersky Endpoint Security v počítači přítomen soubor meicar.exe, aplikace nezjišťuje soubory eicar.com a susp-eicar.com.
  - Aplikace Kaspersky Endpoint Security může nesprávně zobrazovat oznámení o dezinfekci hrozeb. Aplikace může například zobrazovat oznámení o hrozbě pro dříve dezinfikovanou hrozbu.
- Na serverových platformách nejsou podporovány technologie Šifrování na úrovni souborů (FLE) ani Kaspersky Disk Encryption (FDE). Kaspersky Endpoint Security může současně nesprávně zpracovávat události šifrování dat.
- V operačních systémech serveru se nezobrazuje žádné varování týkající se nutnosti pokročilé dezinfekce.
- Z podpory byl vyřazen Microsoft Windows Server 2008. Není podporována instalace aplikace v počítači s operačním systémem Microsoft Windows Server 2008.
- Aplikace Kaspersky Endpoint Security nainstalovaná na serveru s nasazeným nástrojem Microsoft Data Protection Manager (DPM) může způsobit nesprávnou funkci tohoto nástroje. Souvisí to s omezeními provozu DPM. Chcete-li vyloučit nesprávné fungování, měli byste přidat místní jednotky serveru k výjimkám pro součást Ochrana před souborovými hrozbami a úlohy *Kontrola malwaru*.
- Režim Server Core je podporován s omezeními:
  - Místní grafické uživatelské rozhraní není k dispozici, včetně upozornění, vyskakovacích upozornění a dalších ovládacích prvků rozhraní. V aplikaci nelze zobrazit okna s výzvou, včetně následujících oken:
    - výzva k potvrzení verze aplikace a aktualizace modulu;
    - výzva k restartování počítače;
    - dotaz na ověřovací údaje proxy serveru;
    - Výzva k získání přístupu k zařízení (Kontrola zařízení).

- Nejsou k dispozici tyto součásti: Ochrana před webovými hrozbami, Ochrana před hrozbami v poště, Kontrola webu, Ochrana před útoky BadUSB.
- Anti-Bridging není k dispozici.
- Prohlášení o Kaspersky Security Network můžete přijmout pouze v zásadách aplikace v konzole aplikace Kaspersky Security Center.
- Technologie BitLocker Drive Encryption je k dispozici pouze s modulem TPM (Trusted Platform Module). PIN/heslo nelze použít pro šifrování, protože aplikace není schopna zobrazit okno s výzvou k zadání hesla pro ověření před spuštěním. Pokud má operační systém povolený režim kompatibility FIPS (Federal Information Processing Standard), připojte vyměnitelnou jednotku pro uložení šifrovacího klíče, než začnete jednotku šifrovat.

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 dezinfikuje aktivní hrozby bez upozorňování uživatele stejně jako při dezinfekci aktivních hrozeb na serverech. Jelikož operační systém nadále běží v režimu více relací, mohou ostatní aktivní uživatelé přijít o svá data, pokud není hrozba okamžitě vyřešena.
  - 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 s povolenou možností **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 Kaspersky Security Center Network Agent přidejte do konfiguračního souboru následující typy výjimek:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  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.
- Kaspersky Endpoint Security je kompatibilní s hypervizorem VMware ESXi s následujícími omezeními:
  - Aplikace Kaspersky Endpoint Security může být nekompatibilní s ovladači Guest Introspection (vnetWFP.sys, vnetFLT.sys a další). Chcete-li nekompatibilitu vyřešit, aktualizujte ovladače na nejnovější verzi nebo ovladače odinstalujte.
  - V některých případech může být pokus o bezpečné odebrání vyměnitelného disku na virtuálním počítači neúspěšný. Pokuste se zařízení znovu bezpečně odpojit.
- Instalace aplikace Kaspersky Endpoint Security na virtuální počítače pomocí agenta Citrix VDA může skončit chybou kompatibility. K tomu dochází, protože Citrix Provisioning Services má omezenou kompatibilitu s antivirovými řešeními. Osvědčené postupy používání antivirových řešení se službami Citrix Provisioning Services najdete na webu podpory Citrix.
- Kaspersky Endpoint Security přeskočí kontrolu vyměnitelné jednotky, pokud je jednotka připojena k virtuálnímu počítači na hypervizoru Citrix (úloha *Kontrola vyměnitelných jednotek*). V takových zařízeních operační systém zjistí připojenou vyměnitelnou jednotku jako síťovou jednotku. V takových případech můžete použít úlohu *Vlastní kontrola*. Chování aplikace ve standardním režimu a v režimu Light Agent je stejné.

- Pokud je aplikace Kaspersky Endpoint Security nainstalována na virtuálním počítači v infrastruktuře, která používá technologii Citrix App Layering, soubory zjištěné aplikací jako infikované se stavem *Objekt bude při restartu odstraněn* se při restartu počítače automaticky neodeberou.

  Pokud chcete takové soubory odstranit, musíte připojit soubor VHDX obsahující uživatelskou vrstvu do počítače správce vrstvy aplikace Citrix a spustit kontrolu malwaru na připojeném disku.

Kompatibilita s aplikací Kaspersky Security Center

- Ve webové konzole aplikace Kaspersky Security Center verze 14.1 a starší se názvy funkčních oblastí pro součásti Kontrola protokolu a Monitor integrity souborů nezobrazují správně v části nastavení oprávnění pro přístup uživatele ve vlastnostech serveru pro správu.
- Po opravě aplikace je ochrana připojení počítače k serveru pro správu zakázána. Po opravě aplikace spusťte znovu úlohu *Ochrana připojení k serveru pro správu*.
- V aplikaci Kaspersky Security Center 15.1 můžete spouštět úlohy v intervalech několika týdnů (plán **By days of week**). Kaspersky Endpoint Security nepodporuje spouštění úloh ve vícetýdenních intervalech. Pokud máte pro Kaspersky Endpoint Security naplánováno spouštění úlohy v intervalu několika týdnů, aplikace spustí úlohu každý týden v určený den a hodinu.
- V konzole pro správu aplikace Kaspersky Security Center se v okně **Výběr uživatele nebo skupiny uživatelů** zobrazí pouze prvních 50 000 uživatelů ze seznamu uživatelů aplikace Kaspersky Security Center. Další informace najdete v nápovědě k aplikaci Kaspersky Security Center.
- Při hledání spravovaných zařízení v konzole pro správu aplikace Kaspersky Security Center se na kartě **Application components** může současně zobrazovat více variant názvu stejné součásti aplikace, včetně názvů odpovídajících starším verzím aplikace Kaspersky Endpoint Security. Názvy některých součástí mohou být také duplikovány.

  Pro hledání podle součásti stačí vybrat jednu ze zobrazených variant. Další informace o zjišťování zařízení najdete v nápovědě k aplikaci Kaspersky Security Center.

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.
- 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. To je způsobeno tím, že během procesu instalace aplikace nejprve aktivuje vloženou zkušební licenci. Vyžaduje přístup k internetu.
- 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. To je způsobeno tím, že během procesu instalace aktualizace aplikace nejprve aktivuje vloženou zkušební licenci. Vyžaduje přístup 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 14.0, zprávy o výkonu součásti nemusí fungovat správně. Jestliže jste si nainstalovali součásti aplikace Kaspersky Endpoint Security, které nejsou zahrnuty ve vaší licenci, Network Agent může chyby stavu součásti odesílat do protokolu událostí systému Windows. Chcete-li předejít chybám, odeberte součásti, které nejsou zahrnuty ve vaší licenci.

Ochrana před hrozbami v poště

- 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).
- Kaspersky Endpoint Security nepodporuje 64bitovou verzi poštovního klienta aplikace Microsoft Outlook. To znamená, že pokud je v počítači nainstalována 64bitová verze aplikace Microsoft Outlook, aplikace Kaspersky Endpoint Security nekontroluje soubory aplikace Microsoft Outlook (soubory PST a OST), i když je pošta součástí rozsahu kontroly.
- Kaspersky Endpoint Security nepodporuje poštovního klienta Microsoft Outlook New.

Modul pro nápravu

- Aplikace obnoví soubory pouze v zařízeních se souborovým systémem NTFS nebo FAT32.
- Aplikace obnovuje soubory do velikosti 100 MB.
- 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.

Brána firewall

- Pokud pravidlo síťových paketů nebo síťové pravidlo aplikace uvádí názvy DNS, aplikace Kaspersky Endpoint Security může odesílat na server DNS požadavky za účelem zjištění IP adres těchto prostředků. Brána firewall používá adresy IP ke sledování síťové aktivity. Aplikace tedy překládá názvy DNS na IP adresy. Názvy DNS doporučujeme používat v pravidlech pouze pro počítače v LAN nebo interní služby.
- Chcete-li určit pravidlo pro všechny adresy IPv6, přidejte rozsah adres ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Brána firewall nepodporuje masku ::/0.
- 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.
- 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.
- Při importu pravidel paketu brány firewall může aplikace Kaspersky Endpoint Security upravovat názvy pravidel. Aplikace určuje pravidla se shodnými sadami obecných parametrů: protokol, směr, vzdálené a místní porty, doba života paketu (TTL). Pokud je tato sada obených parametrů u více pravidel stejná, aplikace těmto pravidlům přiřadí stejný název nebo připojí k názvu značku parametru. To znamená, že aplikace Kaspersky Endpoint Security importuje všechna pravidla paketů, ale názvy pravidel, která mají stejné obecné parametry, se mohou změnit.
- Pokud jste v síťovém pravidle povolili hlášení událostí aplikace, při přesunu aplikace do jiné skupiny důvěryhodnosti se omezení této skupiny důvěryhodnosti neuplatní. Pokud je tak aplikace ve skupině důvěryhodnosti Důvěryhodné, nebude mít žádná síťová omezení. Poté povolíte hlášení událostí pro tuto aplikaci a přesunete ji do skupiny zabezpečení *Nedůvěryhodné*. Brána firewall nebude u této aplikace vynucovat žádná síťová omezení. Doporučujeme nejdříve aplikaci přesunout do příslušné skupiny zabezpečení a poté povolit hlášení událostí. Pokud vám tento způsob nevyhovuje, můžete pro aplikaci nakonfigurovat omezení ručně v nastavení síťového pravidla. Omezení se vztahuje pouze na místní rozhraní aplikace. Přesouvání aplikace mezi skupinami důvěryhodnosti v příslušné zásadě funguje správně.
- Součásti Brána firewall a Prevence narušení mají stejná nastavení: práva aplikace a chráněné prostředky. Pokud změníte nastavení pro součásti Brána firewall, aplikace Kaspersky Endpoint Security automaticky použije nové nastavení i na součást Prevence narušení. Pokud jste například povolili změny obecného nastavení zásad součásti Brána firewall (zámek je otevřený), bude možné upravovat i nastavení součásti Prevence narušení.
- 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.
- Pokud jste pomocí brány firewall zakázali veškerou síťovou aktivitu, může součást Ochrana před síťovými hrozbami zjistit útok typu Skenování portů. K tomu může dojít, protože aplikace spustí součást Ochrana před síťovými hrozbami před bránou firewall, aby zjistila podezřelou aktivitu v síti.

Ochrana před útoky BadUSB

- Aplikace Kaspersky Endpoint Security resetuje časový limit zámku zařízení USB, když je počítač uzamčen (například vypršel časový limit zámku obrazovky). To znamená, že pokud opakovaně zadáte nesprávný autorizační kód zařízení USB a aplikace toto zařízení USB uzamkne, aplikace Kaspersky Endpoint Security vám umožní opakovat pokus o ověření po odemknutí počítače. V tomto případě aplikace Kaspersky Endpoint Security nezamyká zařízení USB po dobu uvedenou v nastavení součásti Ochrana před útoky BadUSB.
- Aplikace Kaspersky Endpoint Security resetuje časový limit uzamčení zařízení USB, když je ochrana počítače pozastavena. To znamená, že pokud opakovaně zadáte nesprávný autorizační kód zařízení USB a aplikace toto zařízení USB uzamkne, aplikace Kaspersky Endpoint Security vám umožní opakovat pokus o ověření po obnovení ochrany počítače. V tomto případě aplikace Kaspersky Endpoint Security nezamyká zařízení USB po dobu uvedenou v nastavení součásti Ochrana před útoky BadUSB.

Kaspersky Security Network

- Pokud adresa serveru zahrnuje znaky jiné abecedy než latinky (jiné symboly než ASCII), Kaspersky Endpoint Security nepodporuje HTTPS při připojování k proxy serveru KSN (zaškrtnuté políčko **Use HTTPS** v nastavení připojení ke KSN).
- Při přechodu z používání globální služby Kaspersky Security Network na privátní službu Kaspersky Security Network (KPSN) nebo naopak je v aplikaci Kaspersky Security Center v zásadách konkrétního produktu zakázána možnost účastnit se služby Kaspersky Security Network. Po přepnutí si pečlivě přečtěte text Prohlášení o Kaspersky Security Network a potvrďte svůj souhlas s účastí v KSN. Text prohlášení si můžete přečíst v rozhraní aplikace nebo při úpravách zásad produktu.
- Počínaje verzí Kaspersky Endpoint Security 12.9 pro systém Windows je při přechodu z KPSN na globální síť KSN nutné znovu potvrdit souhlas s Prohlášením o Kaspersky Security Network. Za tímto účelem je třeba ve vlastnostech zásad nebo v rozhraní aplikace povolit používání sítě Kaspersky Security Network a potvrdit souhlas s Prohlášením o Kaspersky Security Network. Pokud jste již globální KSN používali, musíte nejprve zakázat používání služby KSN, poté ji znovu povolit a potvrdit souhlas s Prohlášením o Kaspersky Security Network. Pokud s Prohlášením o Kaspersky Security Network nesouhlasíte, aplikace nebude mít přístup k datům ze služby Kaspersky Security Network.
- Kaspersky Endpoint Security neodesílá textové soubory (jako jsou soubory TXT, CSV, LOG a DOCX bez maker) do služby Kaspersky Security Network ke kontrole. Aplikace odesílá na kontrolu do KSN soubory, které mohou představovat hrozbu. Mezi tyto soubory patří spustitelné soubory nebo soubory, které mohou obsahovat spustitelný kód (jako jsou makra v souborech DOCX). Za kontrolu textových souborů jsou odpovědné jiné součásti aplikace. Můžete také ručně zkontrolovat reputaci textového souboru z jeho místní nabídky. Pokud má textový soubor reputaci *Nedůvěryhodné (Kaspersky Security Network)*, aplikace bude ignorovat akci definovanou pro zjištěné hrozby.

Kontrola aplikací

- Při práci s pravidly součásti Kontrola aplikací se nedoporučuje přidávat více než 100 000 celkových podmínek zahrnutí a výjimek pro aplikace v různých kategoriích za předpokladu, že Kaspersky Endpoint Security běží na počítači, který splňuje minimální hardwarové požadavky a funguje na Microsoft Windows 10.
- Při práci s pravidly součásti Kontrola aplikací ve webové konzole aplikace Kaspersky Security Center jsou podporovány pouze archivy ve formátu ZIP. Archivy v jiných formátech, například RAR nebo 7z, nejsou podporovány. Při práci s pravidly součásti Kontrola aplikací v konzole pro správu (MMC) žádné takové omezení neexistuje.
- Při práci s pravidly součásti Kontrola aplikací ve webové konzole aplikace Kaspersky Security Center je maximální podporovaná velikost nahrávaného souboru 104 MB. Při práci s pravidly součásti Kontrola aplikací v konzole pro správu (MMC) žádné takové omezení neexistuje.
- 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.
- Pokud jste při upgradu aplikace Kaspersky Endpoint Security přidali nová *předdefinovaná pravidla součásti Kontrola aplikací*, nelze tato pravidla použít na předchozí verze aplikace.
- Když jsou progresivní webové aplikace (PWA) blokovány součástí Kontrola aplikací, appManifest.xml je v sestavě označen jako blokovaná aplikace.
- Při přidávání standardní aplikace Poznámkový blok do pravidla součásti Kontrola aplikací v systému Windows 11 nedoporučujeme zadávat cestu k aplikaci. Na počítačích se systémem Windows 11 operační systém používá aplikaci Metro Notepad nacházející se zde: `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe`. V předchozích verzích operačního systému se aplikace Poznámkový blok nachází v těchto složkách:
  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

  Při přidávání Poznámkového bloku do pravidla součásti Kontrola aplikací můžete zadat název aplikace a hodnotu hash souboru například z vlastností spuštěné aplikace.

- Když migrujete zásadu KSWS do profilu zásad KES, průvodce hromadným převodem zásad a úloh (průvodce migrací) přejmenuje kategorie aplikací, pokud názvy kategorií obsahují zakázané znaky: `'` `*` `<` `>` `?` `\` `:` `|`. Průvodce migrací tyto znaky nahradí znaky `_`. Například kategorie aplikace `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` se přejmenuje na `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Kontrola zařízení

- Kaspersky Endpoint Security může protokolovat události připojení a odpojení externích zařízení. Služby Windows používají k připojení nebo odpojení zařízení systémový uživatelský účet. Kvůli tomu není možné zjistit, který uživatel zařízení připojuje nebo odpojuje. Aplikace Kaspersky Endpoint Security určí u události uživatelský účet SYSTEM.
- 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.
- 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. Aplikace Kaspersky Endpoint Security registruje události odpojení pouze u následujících typů zařízení: Přenosná zařízení (MTP), Vyměnitelné jednotky, Diskety, Disky CD/DVD. U ostatních typů zařízení aplikace události odpojení neregistruje. Aplikace registruje operaci připojení zařízení k počítači u všech typů zařízení.
- 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.
- Pokud proběhne upgrade aplikace bez restartu počítače, Kontrola zařízení nepoužije pravidla přístupu na zařízení, která se připojí později. Pokud ale bylo zařízení připojeno před upgradem, Kontrola zařízení použije pravidla správně. Aby aplikace správně fungovala u zařízení, která se připojí později, restartujte počítač.
- Na počítačích s nainstalovanou aplikací Kaspersky Endpoint Security verze 12.0 se režim přístupu k tiskárně **Povolit a nezaznamenávat do protokolu** u typu zařízení **Síťové tiskárny** nazývá **V závislosti na sběrnici připojení**, pokud je v počítači použita zásada aplikace Kaspersky Endpoint Security verze 12.1. V těchto režimech aplikace provádí stejné akce. V aplikaci Kaspersky Endpoint Security verze 12.1 je se režim přístupu pro síťové tiskárny správně nazývá **Povolit a nezaznamenávat do protokolu**.
- Počínaje aplikací Kaspersky Endpoint Security 12.0 pro Windows aplikace umožňuje konfiguraci pravidel tisku pro tiskárny (řízení tisku). Po instalaci aplikace s řízením tisku nebo po aktualizaci aplikace na verzi s řízením tisku musíte restartovat počítač. Dokud není počítač restartován, Kaspersky Endpoint Security neuplatňuje pravidla tisku a může řídit pouze přístup k tiskárnám. Pokud restartování počítače nepříznivě ovlivní pracovní postupy ve vaší organizaci, můžete restartovat pouze službu spoolsv (zařazování tisku). Řízení tisku není podporováno na počítačích s architekturou ARM.
- Počínaje aplikací Kaspersky Endpoint Security pro Windows verze 12.0 je protokol WPA3 podporován aplikací pro zařízení typu **Wi-Fi**. Pokud je na počítači aplikována zásada Kaspersky Endpoint Security verze 12.2, na počítačích s Kaspersky Endpoint Security verze 11.11.0 a starší je vybrán protokol WPA2; WPA2/WPA3 je vybrán pro verze 12.0 až 12.1; WPA3 je vybrán pro verze 12.2 a novější.
- Zařízení Apple se klasifikují jako přenosná zařízení (MTP) a zařízení iTunes. Operační systém může připojení zařízení Apple nesprávně identifikovat a neurčit je jako přenosné zařízení (MTP). Zařízení Apple proto nebude k dispozici ve správci souborů, ale bude přístupné v aplikaci iTunes. Kaspersky Endpoint Security tak bude kontrolovat přístup k zařízení Apple pouze v aplikaci iTunes. Pokud chcete k zařízení Apple přistupovat jako k přenosnému zařízení (MTP), musíte přejít do správce zařízení a ze seznamu řadičů USB odebrat ovladač USB mobilního zařízení Apple. Po restartování počítače operační systém identifikuje zařízení Apple jako přenosné zařízení (MTP) a zařízení iTunes. Kaspersky Endpoint Security bude kontrolovat přístup k zařízení v aplikaci iTunes i ve správci souborů.
- V aplikaci Kaspersky Endpoint Security 12.3 pro Windows se nastavení přístupu liší u typu zařízení **Bluetooth**. Pokud jste v předchozí verzi aplikace zadali hodnotu **V závislosti na sběrnici připojení**, po upgradu aplikace na verzi 12.3 se nakonfigurovaná hodnota změní na **Povolit a nezaznamenávat do protokolu**. To nemění chování zařízení.
- Součást Kontrola zařízení podporuje zařízení Bluetooth pouze prostřednictvím sady ovladačů Bluetooth systému Microsoft Windows. Ovládání zařízení nemusí fungovat správně se sadami ovladačů Bluetooth třetích stran.
- Pokud zařízení Bluetooth skrývá nebo falšuje svou třídu zařízení (COD), součást Kontrola zařízení nemusí fungovat správně.
- V počítačích se systémem Windows 7 nebo Windows 8 s určitými ovladači dongle Realtek Bluetooth nemusí být možné povolit připojení zařízení Bluetooth pouze jako vstupních zařízení (třída HID). To znamená, že pokud v nastavení aplikace zakážete přístup k zařízením Bluetooth a přidáte k výjimkám vstupní zařízení, může Kontrola zařízení místo toho zabránit přístupu ke všem zařízením Bluetooth.

Kontrola webu

- Formáty OGV a WEBM nejsou podporovány.
- Protokol RTMP není podporován.

- Kontrola webu podporuje pouze WSL1. Aplikace nekontroluje přenosy WSL2.

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.
- Kaspersky Security Center 15.1 nemůže u konkrétního pravidla vygenerovat podrobnou zprávu **Zpráva o stavu pravidel součásti Adaptivní kontrola anomálií**.

Drive Encryption (FDE)

- Technologie Kaspersky Disk Encryption není podporována na počítačích s architekturou ARM.
- Technologie BitLocker Drive Encryption není podporována v počítačích se systémem Windows Home.
- 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.
- Na jednom šifrovaném počítači nemůže koexistovat více agentů stahování.
- Při pokusu o obnovení bitové kopie spouštěcího disku GPT v nezašifrovaném stavu může operační systém způsobit nefunkčnost operačního systému. Chcete-li se tomu vyhnout, dodržujte tato doporučení:
  - Před obnovením bitové kopie ze zálohy disk plně dešifrujte.
  - Při vytváření bitové kopie použijte kopírování sektor po sektoru.

- Před obnovením bitové kopie odstraňte data z prvních sektorů šifrovaného disku a znovu inicializujte disk.

- 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 `<domain>/<Windows account name>`, po změně názvu počítače musíte také změnit názvy účtů, které byly vytvořeny pro místní uživatele tohoto počítače. Představte si například, že v počítači `Ivanov` je místní uživatel `Ivanov` a pro tohoto uživatele byl vytvořen účet ověřovacího agenta s názvem `Ivanov/Ivanov`. Pokud byl název počítače `Ivanov` změněn na `Ivanov-PC`, musíte změnit název účtu Ověřovacího agenta pro uživatele `Ivanov` z `Ivanov/Ivanov` na `Ivanov-PC/Ivanov`. 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 `Ivanov/Ivanov`).

- 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).

- Šifrování souborů není podporováno na počítačích s architekturou ARM.

- Šifrování souborů a složek není podporováno v operačních systémech Microsoft Windows Embedded.

- Po instalaci aplikace musíte restartovat operační systém, aby šifrování souborů a složek fungovalo správně.

- Aplikace podporuje šifrování souborů pouze na zařízeních se systémem soubor; NTFS a FAT32. Pokud je zašifrovaný soubor přenesen na zařízení s nepodporovaným systémem souborů (například exFAT), soubor na tomto zařízení nebude zašifrován a bude jej možné upravit.
- 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 funkce Encrypting File System 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*.
- Při kopírování dešifrovaného souboru, například na vyměnitelné médium, může soubor zůstat zašifrovaný. Může k tomu dojít, protože když se správce souborů (například explorer.exe) pokusí získat přístup k šifrovanému souboru, uloží hodnotu hash souboru do zvláštního seznamu procesu. Při pokusu správce souborů o přístup k souboru po dešifrování souboru proces hledá v seznamu hodnotu hash souboru. Pokud je hodnota hash nalezena, aplikace Kaspersky Endpoint Security ponechá soubor zašifrovaný. Chcete-li se tomu vyhnout, musíte vymazat seznam procesu. Operační systém automaticky vymaže seznam procesu, jakmile se zaplní. Seznam můžete vyprázdnit také ručně. Chcete-li tak učinit, můžete restartovat počítač, restartovat proces, který používáte pro přístup k souboru (například explorer.exe), nebo můžete použít jiného správce souborů, kterého jste ještě nepoužili pro přístup k šifrovanému souboru.
- 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.
- Než rozbalíte zašifrovaný archiv, ujistěte se, že máte na disku dostatek volného místa pro umístění rozbalených souborů. Pokud na disku nemáte dostatek místa, může být rozbalení archivu dokončeno, ale soubory mohou být poškozeny. V tomto případě je možné, že aplikace Kaspersky Endpoint Security nezobrazí žádné chybové zprávy.
- 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.
- Nemůžete použít Mobilního správce souborů pro přístup k vyměnitelné jednotce, pokud současně platí 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 Mobilního 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.
- Pokud jsou vyměnitelné jednotky šifrovány s podporou přenosného režimu, nelze kontrolu věku hesla deaktivovat.
- 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 CSC (Client-Side Caching) není podporována. Není podporováno šifrování offline souborů ani technologie Branch Caching přes SMB pro servery. 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.
- 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 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.
- Kaspersky Endpoint Security nešifruje soubory, které jsou umístěny v cloudovém úložišti OneDrive nebo v jiných složkách, které mají název OneDrive. Kaspersky Endpoint Security také blokuje kopírování zašifrovaných souborů do složek OneDrive, pokud tyto soubory nejsou přidány do pravidla dešifrování.
- 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).
- Nedoporučujeme šifrovat dočasné soubory, protože to může způsobit ztrátu dat. Například aplikace Microsoft Word vytváří při zpracování dokumentu dočasné soubory. Pokud jsou dočasné soubory zašifrovány, ale původní soubor nikoli, může se uživateli při pokusu o uložení dokumentu zobrazit chyba *Přístup odepřen*. Kromě toho může Microsoft Word soubor uložit, ale příště už nebude možné dokument otevřít, tj. data budou ztracena. Chcete-li zabránit ztrátě dat, musíte z pravidel šifrování vyloučit složku dočasných souborů.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Nemůžete kontrolovat objekt v karanténě v důsledku úlohy *Move file to Quarantine*.
- Do karantény nelze vložit Alternate Data Stream (ADS) větší než 4 MB. Kaspersky Endpoint Security přeskočí ADS této velikosti bez upozorňování uživatele.
- Aplikace Kaspersky Endpoint Security neprovádí úlohy *IOC Scan* na síťových jednotkách, pokud cesta ke složce ve vlastnostech úlohy začíná na písmeno jednotky. Aplikace Kaspersky Endpoint Security podporuje u úloh *IOC Scan* formát cesty UNC pouze u síťových jednotek. Například `\\server\shared_folder`.
- Pro zajištění správného fungování úlohy *IOC Scan* za použití výrazů EmailItem je třeba webový modul plug-in Kaspersky Endpoint Security aktualizovat na nejnovější verzi.
- Na počítačích s architekturou ARM úloha *IOC Scan* podporuje e-mailové soubory pouze z následujících poštovních klientů: 32bitová a 64bitová verze aplikace Outlook 2016 a Outlook 2021, 2024 a 365 pro Arm64.
- Import konfiguračního souboru aplikace skončí chybou, pokud je v konfiguračním souboru povoleno nastavení integrace s řešením Kaspersky Sandbox. Před exportem nastavení aplikace musíte Kaspersky Sandbox zakázat. Poté proveďte export/import. Po importu konfiguračního souboru Kaspersky Sandbox povolte.
- Při importu zásad ze souboru KLP se nepoužije hodnota parametru, která určuje přijetí smluvních podmínek Smlouvy Kaspersky Detection and Response Expert. V důsledku toho po importu zásad aplikace Kaspersky Endpoint Security neplní funkce součásti EDR Agent. Aby součást EDR Agent fungovala, otevřete zásady, změňte libovolný parametr a uložte nastavení zásad.
- Pokud je při provádění úlohy *IOC Scan* zjištěn indikátor narušení, aplikace umístí soubor do karantény pouze po dobu stanovenou parametrem Fileltem. Umístění souboru do karantény na jinou dobu není podporováno.
- Pro správu podrobností o výstraze je nutný webový modul plug-in pro aplikace Kaspersky Endpoint Security pro systém Windows verze 11.7.0 nebo novější. Podrobnosti o výstraze jsou nutné při práci s řešeními Endpoint Detection and Response (EDR Optimum a EDR Expert). Podrobnosti o výstraze jsou k dispozici pouze ve webové konzole aplikace Kaspersky Security Center a cloudové konzole aplikace Kaspersky Security Center.
- Migrace konfigurace [KES+KEA] na konfiguraci [KES+integrovaný agent] může skončit chybou odstranění aplikace Kaspersky Endpoint Agent. Chyba při odstraňování aplikace je v nejnovější verzi aplikace Kaspersky Endpoint Agent opravena. Chcete-li aplikaci Kaspersky Endpoint Agent

odebrat, restartujte počítač a vytvořte úlohu odebrání aplikace.

- Konfigurace [KES+KEA+integrovaný agent] není podporována. Taková konfigurace narušuje interakci mezi aplikacemi a řešením Detection and Response, které je v organizaci nasazeno. Kromě toho může používání aplikace Kaspersky Endpoint Agent a integrovaného agenta ve stejném počítači může vést k duplikaci telemetrie a zvýšenému zatížení počítače a sítě. Po přechodu na konfiguraci [KES+integrovaný agent] zkontrolujte, zda byla z počítače odebrána aplikace Kaspersky Endpoint Agent. Pokud aplikace Kaspersky Endpoint Agent funguje i po migraci, odinstalujte ji ručně (například pomocí úlohy *Uninstall application remotely*).

  Instalační program umožňuje nasadit aplikaci Kaspersky Endpoint Agent v počítači s nainstalovanou aplikací Kaspersky Endpoint Security a integrovaným agentem. Kaspersky Endpoint Agent a integrovaný agent mohou být nainstalovány i na jednom počítači jako výsledek úlohy *Změna součástí aplikace*. Chování závisí na verzi aplikace Kaspersky Endpoint Security a Kaspersky Endpoint Agent.

- Při generování podrobností o výstraze aplikace poskytuje informace o zjištěné hrozbě, včetně hodnot hash upravených souborů. Při generování podrobností výstrahy aplikace Kaspersky Endpoint Security vypočítá hodnotu hash souboru. Uvědomte si, že původní hodnota hash souboru v době vygenerování události úpravy souboru nemusí být stejná jako hodnota hash vypočítaná při vygenerování podrobností o výstraze.

- Pro správu podrobností součástí EDR Optimum a Kaspersky Sandbox je nutný webový modul plug-in pro aplikace Kaspersky Endpoint Security pro systém Windows verze 11.7.0 nebo novější. Pro správu součásti EDR Expert je nutný webový modul plug-in pro aplikace Kaspersky Endpoint Security pro systém Windows verze 11.8.0 nebo novější. Pokud jste vytvořili úlohu *Změna součástí aplikace* pomocí webového modulu plug-in, který nepodporuje práci s těmito součástmi, instalační program tyto součásti na počítačích s nainstalovanou součástí EDR Optimum, EDR Expert nebo Kaspersky Sandbox odstraní.

- Integrovaný agent, EDR (KATA), obnoví síťovou izolaci počítače po restartu počítače, i když doba izolace vypršela. Chcete-li zabránit opakované izolaci počítače, musíte vypnout izolaci sítě v konzole řešení Kaspersky Anti Targeted Attack Platform.

- Po dokončení izolace sítě doporučujeme upgradovat aplikaci. Po upgradu aplikace Kaspersky Endpoint Security lze izolaci sítě zastavit.

- Integrovaní agenti pro EDR (KATA), EDR Optimum a EDR Expert nejsou vzájemně kompatibilní. Aktivaci integrovaného agenta EDR pomocí samostatné licence k doplňku Kaspersky Endpoint Detection and Response lze proto přeskočit, pokud jste aktivovali aplikaci Kaspersky Endpoint Security s jinou funkcí EDR. Například aktivace integrovaného agenta EDR (KATA) se samostatnou licencí se vynechá, pokud jste aktivovali Kaspersky Endpoint Security pomocí licence k řešení [KES+EDR Optimum].

- V aplikaci Kaspersky Endpoint Security verze 12.1 nepodporuje integrovaný agent EDR (KATA) následující metasoubory pro úlohu *Získat metasoubory NTFS*: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Podpora pro tyto metasoubory byla přidána do aplikace Kaspersky Endpoint Security verze 12.2.

- Při migraci z aplikace Kaspersky Endpoint Agent na řešení Kaspersky Endpoint Security pro řešení Kaspersky Anti Targeted Attack Platform (EDR) může dojít k chybám při připojování počítače k serverům součásti Central Node. Důvodem je, že průvodce migrací ve webové konzole přeskočí následující nastavení zásad a nemigruje je:

  - Zákaz změny nastavení **Connection settings** („zámek").

    Ve výchozím nastavení lze nastavení měnit („zámek" je otevřený). Nastavení se proto v počítači nepoužijí. Musíte zakázat změnu nastavení a „zámek" zavřít.

  - Kryptokontejner.

    Pokud pro připojení k serverům Central Node používáte obousměrné ověřování, musíte znovu přidat kryptokontejner. Průvodce migrací správně migruje certifikát serveru TLS.

  Průvodce migrací zásad a úloh v konzole pro správu (MMC) migruje všechna nastavení řešení Kaspersky Anti Targeted Attack Platform (EDR).

- Nesprávně se zobrazuje stav aktivace aplikace, pokud je aplikace nainstalována v režimu Endpoint Detection and Response Agent podporujícím řešení Kaspersky Managed Detection and Response bez připojení k aplikaci Kaspersky Security Center. Po stažení souboru BLOB se v oznamovací oblasti hlavního panelu systému Windows zobrazí nesprávný stav: *Aplikace není aktivována*. V rozhraní aplikace se ale stav aktivace zobrazuje správně. Pro správnou funkci aplikace restartujte počítač.

- Kaspersky Endpoint Security umožňuje integraci s řešením Kaspersky Anti Targeted Attack Platform pomocí součásti EDR (KATA) nebo Endpoint Sensor (nepodporováno). Upozorňujeme, že k interakci s řešením Kaspersky Anti Targeted Attack Platform můžete použít pouze jednu ze součástí. Chcete-li zobrazit stav součásti, otevřete vlastnosti počítače v konzole pro správu (MMC) v části **Applications**, otevřete vlastnosti Kaspersky Endpoint Security pro Windows a přejděte do části **Components**. V souvislosti se zobrazováním stavu součásti pro interakci s řešením Kaspersky Anti Targeted Attack Platform je potřeba vzít v úvahu následující zvláštní aspekty:

  - U modulu plug-in pro správu 12.0 a starších verzí aplikace zobrazuje aktuální stav **Endpoint Sensor**. V aplikaci Kaspersky Endpoint Security 12.0 a dřívějších není součást EDR (KATA) k dispozici. Součást EDR (KATA) byla představena ve verzi 12.1.

  - U modulu plug-in pro správu 12.1 a novějších verzí aplikace zobrazuje celkový stav **Endpoint Detection and Response (KATA)**, což může znamenat buď stav nástroje Endpoint Sensor, nebo stav součásti EDR (KATA). To závisí na verzi aplikace nainstalované v počítači uživatele a dostupných součástech, které můžete použít k interakci s řešením Kaspersky Anti Targeted Attack Platform.

- Počínaje aplikací Kaspersky Endpoint Security verze 12.6 a vyšší nezobrazuje Kaspersky Security Center Web Console verze 14.2 a nižší správně název součásti **Endpoint Detection and Response (KATA)** ve vlastnostech počítače. Namísto **Endpoint Detection and Response (KATA)** aplikace zobrazí název součásti **Endpoint Detection and Response Expert (KATA EDR)**. Chcete-li zobrazit seznam součástí, otevřete vlastnosti počítače ve webové konzole, v části **Applications** otevřete vlastnosti aplikace Kaspersky Endpoint Security pro systém Windows a přejděte do části **Components**. Kaspersky Security Center Web Console od verze 15.1 aplikace zobrazuje název součásti správně.

- Při aktualizaci modulu plug-in pro správu řešení Kaspersky Endpoint Detection and Response na verzi 15.3 nainstalovanou ve webové konzole verze 14.0–14.2 se podrobnosti o výstraze zobrazují nesprávně. Aby podrobnosti o výstraze fungovaly správně, restartujte server pro správu aplikace Kaspersky Security Center.
- Modul plug-in pro správu Kaspersky Endpoint Detection and Response verze 15.4 a novější nepodporuje Kaspersky Security Center verze 14.0. Po aktualizaci modulu plug-in pro správu se podrobnosti o výstraze zobrazují nesprávně.
- Řešení třídy Kaspersky Extended Detection and Response (XDR) verze 1.4 nepodporují webový modul plug-in aplikace Kaspersky Endpoint Security pro systém Windows verze 12.12 a novější. Můžete buď ponechat aktuální verzi webového modulu plug-in, nebo aktualizovat řešení XDR na verzi 2.0 nebo novější.
- Kaspersky Endpoint Security neodesílá objekty určené pro architekturu ARM do součásti Kaspersky Sandbox.
- Integrace s řešením Kaspersky Endpoint Detection and Response Expert není podporována na počítačích s architekturou ARM.

Další omezení

- Operační systémy Windows počínaje verzí 11 24H2 podporují technologii UDP Receive Segment Coalescing Offload (URO). Tato technologie je ve výchozím nastavení povolena, pokud je v počítači nainstalována kompatibilní síťová karta a ovladače. Zakázání URO v počítači uživatele může výrazně snížit výkon aplikace.
- Kaspersky Endpoint Security podporuje podsystém WSL (Windows Subsystem for Linux) s omezeními:
  - WSL 1. Aplikace monitoruje síťový provoz a zjišťuje hrozby prostřednictvím HTTP/HTTPS. Vzhledem k tomu, že aplikace Kaspersky Endpoint Security používá ke kontrole bezpečných připojení HTTPS svůj vlastní certifikát, může dojít k přerušení provozu některých aplikací třetích stran.
  - WSL 2. Aplikace nepodporuje WSL 2.
- 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.
- Webové adresy, které jsou přidány do seznamu důvěryhodných, mohou být nesprávně zpracovány.
- V konzole aplikace Kaspersky Security Center nelze uložit soubor na disk ze složky **Advanced** → **Repositories** → **Active threats**. Chcete-li soubor uložit, musíte infikovaný soubor dezinfikovat. Při dezinfekci aplikace uloží kopii souboru do zálohy. Nově můžete soubor uložit na disk ze složky **Advanced** → **Repositories** → **Backup**.
- Dědičnost nastavení přenosu dat na server pro správu (**Obecná nastavení** → **Zprávy a úložiště** → **Přenos dat na server pro správu**) se liší od dědičnosti jiných nastavení. Pokud jste v zásadě povolili změnu nastavení přenosu dat („zámek" je otevřený), tato nastavení budou resetována na výchozí hodnoty ve vlastnostech místního počítače v konzole, pokud nebyla dříve definována. Pokud byla tato nastavení definována dříve, jejich hodnoty budou obnoveny. Při odstranění zásady se nastavení dědí stejným způsobem. V těchto případech se ostatní nastavení ve vlastnostech místního počítače dědí ze zásady.
- 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.
- Aplikace Kaspersky Endpoint Security zabraňuje komunikaci prostřednictvím protokolu QUIC. Prohlížeče používají standardní přenosový protokol (TLS nebo SSL) bez ohledu na to, zda je v prohlížeči povolena podpora QUIC.
- Když software třetí strany spolupracuje s knihovnou Libcurl, může dojít k chybám připojení TLS. To může souviset s certifikátem Kaspersky, který aplikace Kaspersky Endpoint Security používá ke kontrole šifrovaných připojení. Chcete-li pokračovat v práci, můžete zakázat ověřování certifikátů pro software třetích stran (nedoporučuje se) nebo přidat tělo certifikátu Kaspersky do úložiště certifikátů cURL. Podrobné informace naleznete ve znalostní bázi společnosti Kaspersky.
- 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.
- 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 aplikaci a ve zprávě Kaspersky Security Center.
- Zpráva Kaspersky Security Center 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.
- V cloudové konzole aplikace Kaspersky Security Center nelze povolit zobrazení všech položek zprávy. Ve webové konzole můžete pouze změnit počet položek zobrazovaných ve zprávách. Standardně se ve webové konzole aplikace Kaspersky Security Center zobrazuje 1000 položek

zprávy. Zobrazení více položek zprávy můžete povolit v konzole pro správu.

- V konzole aplikace Kaspersky Security Center nelze nastavit zobrazení více než 1000 položek zprávy. Pokud nastavíte hodnotu vyšší než 1000, v konzole aplikace Kaspersky Security Center se zobrazí pouze 1000 položek zprávy.
- 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 Windows.
- Nemůžeme zaručit, že ovládání zvuku bude fungovat před prvním restartem po instalaci aplikace.
- V konzole pro správu v nastavení součásti Prevence narušení v okně pro konfiguraci oprávnění aplikace není tlačítko **Odebrat** k dispozici. Aplikaci můžete odebrat ze skupiny důvěryhodnosti prostřednictvím místní nabídky aplikace.
- V místním rozhraní aplikace v nastavení součásti Narušení hostitele nejsou oprávnění aplikace a chráněné prostředky dostupné k zobrazení, pokud počítač spravuje zásada. Nejsou k dispozici ovládací prvky pro posouvání, vyhledávání, filtrování a další ovládání okna. Oprávnění aplikace zobrazíte ve vlastnostech zásad v konzole aplikace Kaspersky Security Center.
- 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.
- U procesů PICO není podporováno protokolování výpisu paměti.
- 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:\folder1\folder2`, bude spuštěna kontrola pro cestu `C:\folder1\`.
- Pokud používáte zásady omezení softwaru (Software Restriction Policies, SRP), počítač se nemusí načíst (černá obrazovka). Abyste předešli nesprávnému fungování, musíte ve vlastnostech SRP povolit použití knihoven aplikací. Ve vlastnostech SRP přidejte pravidlo s úrovní zabezpečený **Neomezené** pro soubor khkum.dll (položka nabídky **Nové pravidlo hash**). Soubor se nachází ve složce `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.0\klhk\klhk_x64\`. Pokud jste vybrali tento postup, musíte ještě zrušit zaškrtnutí políčka **Stahovat aktualizace modulů aplikace** v nastavení úlohy *Aktualizace* pro Kaspersky Endpoint Security. Podrobnosti o používání SRP najdete v dokumentaci společnosti Microsoft.

  Můžete také deaktivovat SRP a používat pro řízení používání aplikací součást Kontrola aplikací aplikace Kaspersky Endpoint Security.
- Pokud počítač patří do domény v rámci objektu zásad skupiny systému Windows (Group Policy Object, GPO) s parametrem DriverLoadPolicy nastaveným na hodnotu 8 (Good only), způsobí restartování počítače s nainstalovanou aplikací Kaspersky Endpoint Security chybu BSOD. Chcete-li zabránit chybě, musí být parametr Early Launch Antimalware (ELAM) v zásadách skupiny nastaven na hodnotu 1 (Good and unknown). Nastavení ELAM se nachází v zásadách v části **Computer Configuration** → **Administrative Templates** → **System** → **Early Launch Antimalware**.
- 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.

- 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).

- Pokud je aplikace Kaspersky Endpoint Security nainstalována na serveru SQL Server DBMS, aplikace odešle požadavky do instance serveru. To je nutné při kontrole úloh součásti SQL Server Agent a k zabránění spouštění škodlivých úloh. Aplikace Kaspersky Endpoint Security používá pro úlohy kontroly uživatelský účet SQL Server. Aplikace odešle požadavky na server při kontrole systémové paměti a po aktualizaci antivirových databází.

- Kompatibilita aplikace Kaspersky Endpoint Security a softwarem Secret Net Studio je omezená:

  - Aplikace Kaspersky Endpoint Security není kompatibilní se součástí Antivirus softwaru Secret Net Studio.

    Aplikaci nelze nainstalovat do počítače, kde je nasazen software Secret Net Studio se součástí Antivirus. Aby byla interoperabilita možná, musíte součást Antivirus ze softwaru Secret Net Studio odebrat.

  - Aplikace Kaspersky Endpoint Security není kompatibilní se součástí Ochrana disku a šifrování dat softwaru Secret Net Studio.

    Aplikaci nelze nainstalovat do počítače, kde je nasazen software Secret Net Studio se součástí Ochrana disku a šifrování dat. Aby byla interoperabilita možná, musíte součást Ochrana disku a šifrování dat ze softwaru Secret Net Studio odebrat.

  - Secret Net Studio není kompatibilní se součástí File Level Encryption (FLE) aplikace Kaspersky Endpoint Security.

    Když nainstalujete Kaspersky Endpoint Security se součástí File Level Encryption (FLE), Secret Net Studio může fungovat s chybami. Chcete-li zajistit interoperabilitu, musíte z aplikace Kaspersky Endpoint Security součást File Level Encryption (FLE) odebrat.

- Při importu pravidel součásti Monitorování integrity systému aplikace zkontroluje ID a název pravidla. Pokud jsou ID pravidel stejná, Kaspersky Endpoint Security nahradí stávající pravidla novým pravidlem. Při exportu pravidel aplikace automaticky přiřadí ID. Pravidlo s identickými ID může existovat, například pokud jste ručně upravili exportované soubory XML pravidel. Pokud jsou ID pravidel jedinečná, ale názvy pravidel jsou stejné, Kaspersky Endpoint Security přidá k názvu pravidla `(1)` a tak dále.

- Počínaje verzí 12.11 v aplikaci Kaspersky Endpoint Security pro systém Windows není možné zobrazit nastavení nadřazené zásady, která je otevřena v podřízené skupině, ve webové konzole. Ve webové konzole se také zobrazuje varování: *This policy is inherited. You can edit the policy settings only in the administration group in which it was created.*

- Místní oznámení delší než 256 znaků se v konzole pro správu (MMC) nezobrazují.

- Názvy součástí v zásadách a v instalačním balíčku se mohou lišit. Například Endpoint Detection and Response Expert (on-premise) se může jmenovat Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premise) nebo Kaspersky Anti Targeted Attack Platform Integration. Názvy součástí se také mohou lišit v závislosti na verzi aplikace.

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.

Cloud Discovery

Cloud Discovery spravuje přístup uživatelů ke cloudovým službám. Mezi cloudové služby patří například Microsoft Teams, Salesforce nebo Microsoft Office 365. Cloudové služby jsou seskupeny do kategorií, například *Sdílení souborů*, *Messengery* nebo *E-mail*.

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.

Integrační server

Součást Kaspersky Endpoint Security for Virtualization Light Agent. Interaguje mezi součástmi aplikace Kaspersky Endpoint Security a virtuální infrastrukturou.

IOC

Indikátor narušení. Sada dat o škodlivém objektu nebo aktivitě.

Licenční certifikát

Dokument, který společnost Kaspersky přenáší na uživatele společně se souborem klíče nebo aktivačním kódem. Obsahuje informace o licenci udělené uživateli.

Light Agent

Součást Kaspersky Endpoint Security for Virtualization Light Agent. Instaluje se na každý virtuální počítač, který je třeba chránit.

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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` samotné. 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, 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.Example.com\.

Normalizovaná forma adresy: www.example.com.

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.

OpenIOC

Otevřený standard popisů indikátoru narušení (IOC) založený na XML a zahrnující více než 500 různých indikátorů narušení.

Ověřovací agent

Rozhraní umožňující dokončení ověřování pro přístup k šifrovaným pevným diskům a načtení operačního systému po zašifrování spustitelného pevného disku.

Ověřování protokolem Kerberos

Mechanismus vzájemného ověření klienta a serveru před navázáním připojení mezi nimi, který umožňuje komunikaci přes nezabezpečené sítě. Mechanismus je založen na tiketu, který uživatel získá od důvěryhodného ověřovacího centra.

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.

Soubor IOC

Soubor obsahující sadu indikátorů narušení (IOC), které se aplikace pokusí porovnat, aby započítala detekci. Pravděpodobnost detekce může být vyšší, pokud jsou pro objekt v důsledku kontroly nalezeny přesné shody s více soubory IOC.

SVM

Bezpečný virtuální počítač – zvláštní virtuální počítač, na kterém je nainstalována služba scanserver (Server pro ochranu, součást aplikace Kaspersky Endpoint Security for Virtualization Light Agent).

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

Součást Ochrana před souborovými hrozbami umožňuje zabránit infekci systému souborů počítače. Ve výchozím nastavení je součást Ochrana před souborovými hrozbami trvale umístěna v paměti RAM počítače a v reálném čase kontroluje všechny otevřené, uložené a spuštěné soubory. Součást kontroluje soubory na všech jednotkách počítače včetně připojených jednotek. 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 cloudovém úložišti 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 souborů *(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)*	**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 zkontroluje pouze infikovatelné soubory. Před kontrolou souboru, zda neobsahuje škodlivý kód, bude analyzováno interní záhlaví souboru, 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 zkontroluje pouze infikovatelné soubory. Formát souboru je poté určen na základě přípony souboru.
Rozsah kontroly	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 můžete vyloučit pouze 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 se automaticky pokusí dezinfikovat nalezený infikovaný soubor. Pokud se dezinfekce nezdaří, aplikace soubor 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 se dezinfekce nezdaří, aplikace Kaspersky Endpoint Security soubory zablokuje (pro čtení/zápis).

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 záložní kopii souboru pro případ, že byste jej chtěli obnovit nebo pokud jej bude možné v budoucnu dezinfikovat.

Kontrolovat pouze nové a upravené 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

Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).

Kontrolovat distribuční balíčky

Kontrola distribučních balíčků aplikací 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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.

Kontrolovat soubory v poštovním formátu

Kontrolovat soubory v poštovním formátu. Aplikace kontroluje soubory MSG a EML. Soubory v poštovním formátu zahrnují také objekty OLE a soubory MHT. Aplikace Kaspersky Endpoint Security kontroluje soubory ve formátu e-mailu, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.

Nerozbalovat velké složené soubory

Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu.

Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí.

Aplikace kontroluje velké soubory rozbalené z archivů bez ohledu na to, zda je toto políčko zaškrtnuté nebo ne.

Rozbalovat složené soubory na pozadí

Je-li toto políčko zaškrtnuto, aplikace 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 umožní přístup ke složeným souborům, které jsou menší než tato hodnota, až po rozbalení a kontrole těchto souborů.

Není-li toto políčko zaškrtnuto, aplikace umožní přístup ke složeným souborům pouze po rozbalení a kontrole souborů jakékoli velikosti.

Režim kontroly

(k dispozici pouze v konzole pro správu (MMC) a v rozhraní aplikace Kaspersky Endpoint Security)

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.

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 provedení. V tomto režimu kontroluje součást Ochrana před souborovými hrozbami objekty pouze při pokusu o jejich spuštění.

Používat technologii 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.

Používat technologii 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.
Kontrola operací se soubory prováděných v kontejnerech systému Windows	Pokud je uvnitř kontejneru zjištěna hrozba, aplikace použije akci vybranou pro součást Ochrana před souborovými hrozbami. **V případě chyby dezinfekce zastavit kontejner**. Aplikace u zjištěného objektu pravděpodobně nemá dostatečná práva pro čtení a zápis. V takovém případě je dezinfekce nebo odstranění zjištěného objektu nemožná. Je-li toto políčko zaškrtnuto, aplikace zablokuje zjištěný objekt a zastaví kontejner. Není-li toto políčko zaškrtnuto, aplikace zablokuje pouze zjištěný objekt. **Nekontrolovat operace se soubory prováděné v kontejnerech systému Windows**. Je-li toto políčko zaškrtnuto, aplikace kontroluje kontejner pouze při jeho spuštění. Pokud toto políčko není zaškrtnuté, aplikace kontroluje kontejner nepřetržitě v reálném čase.

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.

Chcete-li používat součást Ochrana před webovými hrozbami, musíte provést počáteční konfiguraci aplikace:

- Pro monitorování provozu HTTPS povolte kontrolu šifrovaných připojení (ve výchozím nastavení povolena).
- Vyberte porty, které aplikace Kaspersky Endpoint Security má monitorovat (ve výchozím nastavení aplikace monitoruje všechny porty).
- Vyberte aplikace, jejichž provoz má aplikace Kaspersky Endpoint Security sledovat. Většina prohlížečů se již nachází v seznamu aplikací doporučených společností Kaspersky. Pokud váš prohlížeč v seznamu chybí, přidejte jej ručně.
- Doporučujeme vložit do webového provozu skript interakce s webovou stránkou (ve výchozím nastavení je vkládání skriptů zakázáno). Tento skript umožňuje evidenci událostí součásti Ochrana před webovými hrozbami pro protokol událostí aplikace, protokol událostí OS a zprávy.

Když se uživatel pokusí otevřít škodlivý nebo phishingový web, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění.

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 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 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**. 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 webovou adresu s databází škodlivých webových adres	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.

(k dispozici pouze v konzole pro správu (MMC) a v rozhraní 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 webovou adresu s databází phishingových webových adres *(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 vybrána tato možnost, 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. Můžete také vytvořit obecný seznam výjimek pro šifrovaná připojení. V tomto případě Kaspersky Endpoint Security nekontroluje HTTPS provoz důvěryhodných webových adres, když součásti Ochrana před webovými hrozbami, Ochrana před hrozbami v poště a Kontrola webu vykonávají svoji práci.

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 poskytuje ochranu počítače pomocí antivirových databází, cloudové služby Kaspersky Security Network a heuristické analýzy.

Ochrana před hrozbami v poště může kontrolovat příchozí i odchozí zprávy. Aplikace podporuje POP3, SMTP, IMAP a NNTP v následujících poštovních klientech:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Pokud chcete kontrolovat provoz v poštovních klientech Mozilla Thunderbird, MyOffice Mail a R7-Office Organizer, musíte přidat certifikát Kaspersky do úložiště certifikátů a vybrat vlastní úložiště certifikátů.

Ochrana před hrozbami v poště nepodporuje jiné protokoly a poštovní klienty.

Ochrana před hrozbami v poště nemusí být vždy schopna získat přístup ke zprávám na *úrovni protokolu* (například při použití řešení Microsoft Exchange). Z tohoto důvodu Ochrana před hrozbami pošty zahrnuje rozšíření pro Microsoft Office Outlook. Rozšíření umožňuje kontrolu zpráv na *úrovni poštovního klienta*. Rozšíření Ochrana před hrozbami v poště podporuje 32bitové verze aplikace Outlook 2010, 2013, 2016, 2019, 2021, 2024 a 365. V počítačích s architekturou ARM podporuje rozšíření Ochrana před hrozbami v poště 32bitové verze aplikace Outlook 2016, Outlook 2021, Outlook 2024 a Outlook 365 pro Arm64.

Součást Ochrana před hrozbami v poště nekontroluje zprávy, pokud je poštovní klient otevřen v prohlížeči.

Když je v příloze zjištěn škodlivý soubor, aplikace Kaspersky Endpoint Security přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

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 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 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 tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud objekt nelze dezinfikovat, aplikace infikovaný objekt odstraní. Aplikace přidá do předmětu zprávy informace o provedené akci, například *[Zpráva byla zpracována] <předmět zprávy>*.

Dezinfikovat; a pokud se dezinfekce nezdaří, tak zablokovat. Pokud je v příchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Uživatel bude mít přístup ke zprávě s bezpečnou přílohou. Pokud nelze objekt dezinfikovat, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, pokusí se aplikace tento objekt dezinfikovat. Pokud objekt nelze dezinfikovat, aplikace zablokuje přenos zprávy a poštovní klient zobrazí chybu.

Blokovat. Pokud je v příchozí zprávě zjištěn infikovaný objekt, přidá aplikace k předmětu zprávy varování. Uživatel bude mít k dispozici zprávu se původní přílohou. Pokud je v odchozí zprávě zjištěn infikovaný objekt, aplikace 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

Kontrola dat přenášených prostřednictvím protokolů POP3, SMTP, NNTP a IMAP pomocí součásti Ochrana před hrozbami v poště.

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 Cached Exchange Mode. 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

Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).

> Pokud aplikace 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.

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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.

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 na kontrolu archivů na N sec

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* (také nazývaná Intrusion Detection System, IDS) monitoruje příchozí síťový provoz a sleduje aktivitu charakteristickou pro síťové útoky. Pokud aplikace 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. 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
Považovat skenování portů a přehlcení sítě za útoky	*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. Pokud je detekován útok, aplikace upozorní uživatele a odešle odpovídající událost do aplikace Kaspersky Security Center. Aplikace poskytuje informace o útočícím počítači, které jsou nutné pro včasné akce reakce na hrozby. 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.
Blokovat útočící zařízení po dobu N min	Pokud je tato možnost povolena, 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. Minimální doba, kterou musí útočící počítač strávit na seznamu blokovaných počítačů, je jedna minuta. Maximální doba je 999 minut. 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. Můžete přidat IP adresu s určeným portem a protokolem. Aplikace nezaznamená do protokolu informace o síťových útocích z IP adres, které jsou v seznamu výjimek.
Ochrana před falšováním adresy 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

Součást 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 součást Network Agent. Brána firewall automaticky vytváří pravidla sítě požadovaná pro fungování aplikace a Network Agent. 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, najdete 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 aplikací*. 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 zabezpečení: *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 důvěryhodnosti *Vysoké omezení* 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.

Síťová pravidla pro aplikace fungují určitým způsobem. Síťové pravidlo pro aplikace zahrnuje pravidla přístupu na základě stavu sítě: *Veřejná síť*, *Místní síť*, *Důvěryhodná síť*. Například aplikace ve skupině důvěryhodnosti *Vysoké omezení* 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.

Typy síťového připojení

Brána firewall umožňuje řídit síťovou aktivitu v závislosti na typu síťového připojení. Aplikace Kaspersky Endpoint Security přijímá typ síťového připojení z operačního systému počítače. Typ síťového připojení v operačním systému nastavuje uživatel při nastavování připojení. Typ síťového připojení můžete změnit v nastavení aplikace Kaspersky Endpoint Security. Brána firewall bude sledovat aktivitu sítě v závislosti na typu sítě zadaného v nastavení aplikace Kaspersky Endpoint Security, a ne v operačním systému.

K dispozici jsou následující typy 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.

  Brána firewall ve výchozím nastavení přiřadí internetu typ *Veřejná síť*. Typ 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 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.
Dostupné sítě	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 pro aplikace	**Aplikace**. 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 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 klávesnice 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 opětovné autorizaci této klávesnice.

Pokud číselný kód zadáte nesprávně, aplikace vygeneruje nový kód. Můžete nakonfigurovat počet pokusů o zadání numerického kódu. Pokud byl numerický kód zadán vícekrát nesprávně nebo bylo zavřeno okno autorizace klávesnice (viz obrázek níže), aplikace zablokuje vstup z této klávesnice. Když vyprší doba blokování zařízení USB 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

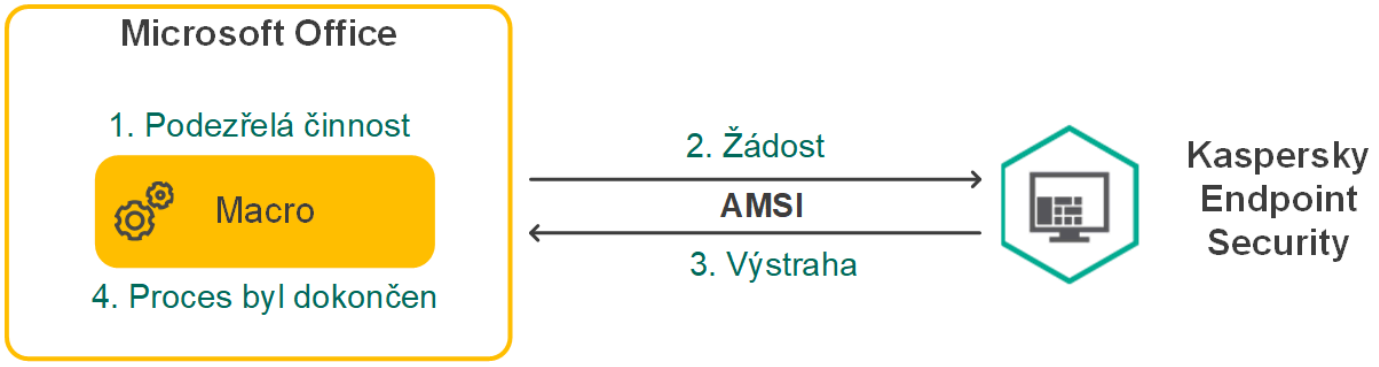
Nastavení součásti Ochrana před útoky BadUSB

Parametr	Popis
Zakázat klávesnici na obrazovce pro ověřování zařízení USB	Pokud je tento přepínač zapnutý, aplikace blokuje použití klávesnice na obrazovce pro ověřování USB zařízení, ze kterého nelze ověřovací kód zadat.
Zakázat používání čárového kódu k autorizaci zařízení USB	Pokud je tento přepínač povolen, aplikace nezobrazuje čárový kód v oznámení o autentizaci čtečky čárových kódů.
Maximální počet pokusů o ověření zařízení USB	Automatické blokování zařízení USB, pokud je zadaný ověřovací kód nesprávně zadán několikrát. Platné hodnoty jsou 1 až 10. Pokud například povolíte pět pokusů o zadání ověřovacího kódu, aplikace zařízení USB po pátém neúspěšném pokusu zablokuje. Aplikace Kaspersky Endpoint Security zobrazí dobu blokování zařízení USB. Po uplynutí této doby máte pět pokusů o zadání ověřovacího kódu.
Časový limit při dosažení maximálního počtu pokusů	Doba blokování zařízení USB po zadaném počtu neúspěšných pokusů o zadání ověřovacího kódu. Platné hodnoty jsou 1 až 180 (minuty).

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 upozornění na hrozbu nepovolí provedení škodlivých akcí (například akci 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 neodmítá požadavky od aplikací třetích stran, pro které je povolena nepřetržitá integrace 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 / více relací Enterprise;

- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows Server 2016 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2019 Essentials / Standard / Datacenter (včetně režimu Server Core);
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (včetně režimu Server Core);
- Windows Server 2025 Standard / Datacenter.

Nastavení ochrany AMSI

Parametr	Popis
Kontrolovat archivy	Kontrola formátů ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE a dalších archivů. Aplikace kontroluje archivy nejen podle přípony, ale i podle formátu. Při kontrole archivů provádí aplikace rekurzivní rozbalování. To umožňuje odhalit hrozby uvnitř víceúrovňových archivů (archiv v archivu).
Kontrolovat distribuční balíčky	Kontrola distribučních balíčků aplikací 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. Aplikace kontroluje soubory formátu Office, které jsou menší než 1 MB, bez ohledu na to, zda je zaškrtávací políčko zaškrtnuto či nikoli.
Nerozbalovat velké složené soubory	Je-li toto políčko zaškrtnuto, aplikace nezkontroluje složené soubory, pokud jejich velikost překračuje zadanou hodnotu. Pokud políčko zaškrtnuté není, aplikace zkontroluje složené soubory všech velikostí. Aplikace 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.

Součást Prevence zneužití navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

Nastavení součásti Prevence zneužití

Parametr	Popis
Při zjištění zneužití	**Blokovat**. 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.
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 je založeno na podpisech BSS a poskytuje aktivní ochranu počítače.

Součást Detekce chování navíc monitoruje síťové porty, zda se v nich nevyskytují procesy aplikací, které mohou ohrozit zabezpečení počítače. Informace o těchto procesech získává aplikace pomocí antivirových databází.

Nastavení součásti Detekce chování

Parametr	Popis
Akce při detekci aktivity malwaru	**Odstranit**. 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. **Blokovat**. 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.

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 (například soubory a aplikace)

Síťová aktivita aplikací je ovládána součástí Brána 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 zabezpečení: *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 *Vysoké omezení* 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	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**. Tabulka přístupových práv ke zdrojům operačního systému a osobním údajům pro aplikace patřící do skupiny důvěryhodnosti. • **Práva**. Tabulka přístupových práv pro procesy a prostředky operačního systému pro aplikace patřící 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 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	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.
Skupina důvěryhodnosti pro aplikace spuštěné před aplikací Kaspersky Endpoint Security	Skupina důvěryhodnosti, do které aplikace Kaspersky Endpoint Security umísťuje aplikace spuštěné před touto aplikací.

Aktualizovat pravidla pro dříve neznámé aplikace ze služby KSN	Pokud je toto políčko zaškrtnuto, bude součást Prevence narušení hostitele aktualizovat práva pro dříve neznámé aplikace pomocí databáze Kaspersky Security Network.
Důvěřovat digitálně podepsaným aplikacím	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 pravidla u aplikací, které nebyly spuštěny déle než N dny (od 1 do 90)	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 nejsou součástí jiných skupin	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 kontroly malwaru.

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.

Kaspersky Security Network



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.

Funkce KSN nemusí být v softwaru dostupná na území USA.

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 reputaci kontrolovaných webových adres a také informace o reputaci kategorii a reputaci kontrolovaných souborů.

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 Kaspersky Security Network a na webových stránkách společnosti Kaspersky. Soubor ksn_<ID jazyka>.txt s textem prohlášení o Kaspersky Security Network je součástí distribučního balíčku aplikace.

Infrastruktura databází reputace společnosti Kaspersky

Kaspersky Endpoint Security podporuje následující infrastrukturní řešení pro práci s databázemi reputace Kaspersky:

- *Kaspersky Security Network (KSN)* je řešení, které používá většina aplikací Kaspersky. Účastníci služby KSN získávají od společnosti Kaspersky informace a odesílají společnosti Kaspersky informace o objektech zjištěných v počítači uživatele, které budou dodatečně analyzovány analytiky společnosti Kaspersky a budou zařazeny do databází reputace a statistik.
- *Kaspersky Private Security Network (KPSN)* 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 KPSN 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.

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

Režim cloudu 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 jako proxy server KSN server pro správu

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

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.

Použít servery KSN, pokud není proxy server KSN 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 KSN Proxy. Servery KSN mohou být umístěny na straně společnosti Kaspersky a u třetí strany (při použití služby Kaspersky Private Security Network).

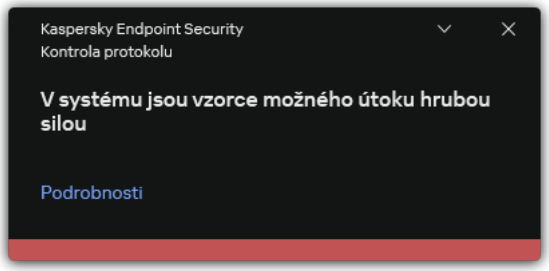
Kontrola protokolu

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice.

Od verze 11.11.0 zahrnuje aplikace Kaspersky Endpoint Security pro systém Windows součást Kontrola protokolu. Kontrola protokolu monitoruje integritu chráněného prostředí na základě analýzy protokolu událostí systému Windows. Pokud aplikace zjistí známky netypického chování systému, informuje o tom správce, protože toto chování může znamenat pokus o kybernetický útok.

Kaspersky Endpoint Security analyzuje protokoly událostí systému Windows a v souladu s pravidly zjišťuje porušení. Součást zahrnuje předdefinovaná pravidla. Předdefinovaná pravidla jsou založena na heuristické analýze. Můžete také přidat vlastní pravidla (vlastní pravidla). Když se pravidlo spustí, aplikace vytvoří událost se stavem *Critical* (viz obrázek níže).

Pokud chcete používat součást Kontrola protokolu, ujistěte se, že je nakonfigurováno nastavení zabezpečení zásad auditu a že systém zaznamenává do protokolu příslušné události (podrobnosti najdete na webu technické podpory společnosti Microsoft).



Upozornění součásti Kontrola protokolu

Nastavení kontroly protokolu

Parametr	Popis
Předdefinovaná pravidla	Seznam pravidel součásti Kontrola protokolu. Předdefinovaná pravidla zahrnují šablony abnormální aktivity v chráněném počítači. Abnormální aktivita může znamenat pokus o útok.
Vlastní pravidla	Seznam pravidel součásti Kontrola protokolu přidaných uživatelem. Můžete si nastavit vlastní kritéria pro aktivaci pravidel součásti Kontrola protokolu. K tomu musíte zadat ID události a vybrat zdroj události. Zdroj událostí můžete vybrat ze standardních protokolů: *Application*, *Security* nebo *System*. Můžete rovněž zadat protokol aplikace třetí strany.

Anti-Cryptor

Součást Anti-Cryptor 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.

Nastavení součásti Anti-Cryptor

Parametr	Popis
Výjimky podle názvu nebo IP adresy	**Výjimky podle názvu nebo IP adresy**. 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. **Výjimky podle masky**. Výjimky z rozsahu ochrany. Vyloučení složky z rozsahu ochrany 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. 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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.
Akce při zjištění hrozby	• **Informovat**. Pokud je vybrána tato možnost, při zjištění pokusu o úpravu souborů ve sdílených složkách aplikace Kaspersky Endpoint Security přidá informace o tomto pokusu o úpravu seznamu aktivních hrozeb, přidá položku do zprávy o místním rozhraní aplikace a odešle informace o zjištěné škodlivé aktivitě do aplikace Kaspersky Security Center. • **Blokovat připojení po dobu (min.) N minut**. Je-li tato možnost vybrána, když aplikace Kaspersky Endpoint Security detekuje pokus o úpravu souborů ve sdílených složkách, zablokuje přístup k úpravám souborů pro relaci, která škodlivou aktivitu iniciovala, a vytvoří záložní kopie upravených souborů.

Pokud je povolena součást Modul pro nápravu a je zaškrtnuta možnost **Blokovat připojení po dobu (min.) N minut**, změněné soubory se obnoví ze záložních kopií.

Rozsah ochrany

Rozsah ochrany je seznam cest ke sdíleným složkám, ve kterých aplikace Kaspersky Endpoint Security monitoruje aktivitu souborů. Při zadávání masky podporuje aplikace Kaspersky Endpoint Security proměnné prostředí a znaky `*` a `?`. Ve výchozím nastavení aplikace automaticky identifikuje sdílené složky a monitoruje aktivitu souborů ve všech složkách.

Kontrola webu

Součást 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).

Chcete-li používat součást Kontrola webu, musíte provést počáteční konfiguraci aplikace:

- Pro monitorování provozu HTTPS povolte kontrolu šifrovaných připojení (ve výchozím nastavení povolena).
- Vyberte porty, které aplikace Kaspersky Endpoint Security má monitorovat (ve výchozím nastavení aplikace monitoruje všechny porty).
- Vyberte aplikace, jejichž provoz má aplikace Kaspersky Endpoint Security sledovat. Většina prohlížečů se již nachází v seznamu aplikací doporučených společností Kaspersky. Pokud váš prohlížeč v seznamu chybí, přidejte jej ručně.
- Doporučujeme vložit do webového provozu skript interakce s webovou stránkou (ve výchozím nastavení je vkládání skriptů zakázáno). Tento skript umožňuje evidenci událostí součásti Kontrola webu pro protokol událostí aplikace, protokol událostí OS a zprávy.

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 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 „*Grafika*“.

- **Jednotlivé adresy**. Můžete zadat webovou adresu nebo použít masky.

Pro regulaci přístupu na webové stránky můžete současně použít několik způsobů. Můžete například omezit přístup k typu dat *Soubory kancelářských aplikací* pouze pro kategorii webu *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.

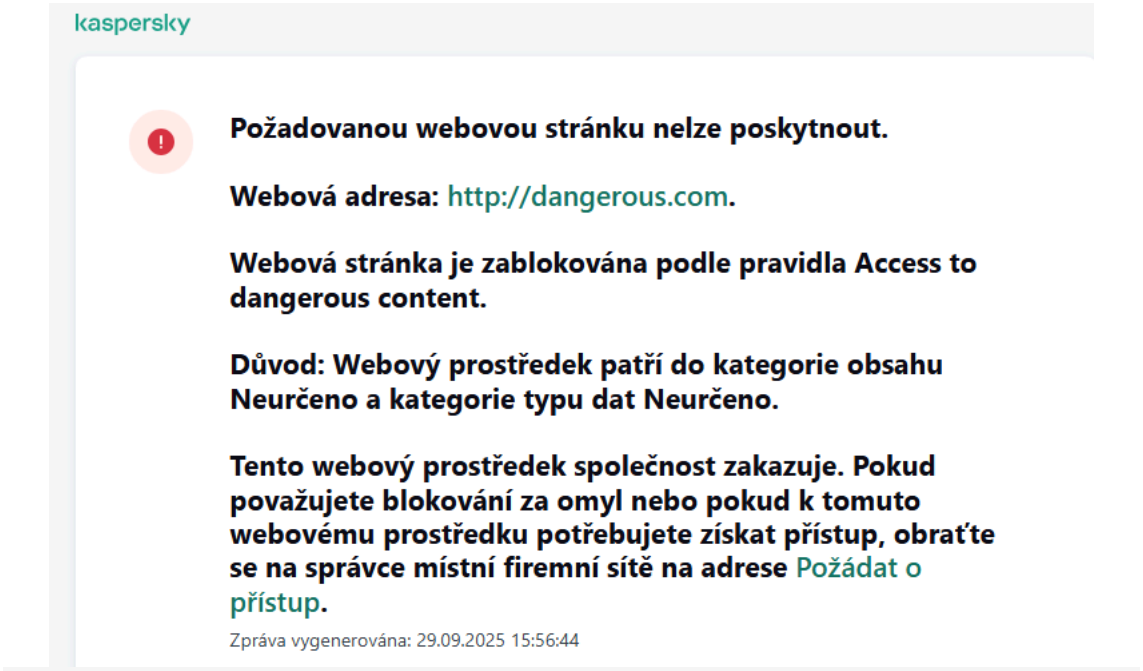
  Můžete například omezit přístup k internetu prostřednictvím prohlížeče pro všechny uživatele společnosti kromě IT oddělení.

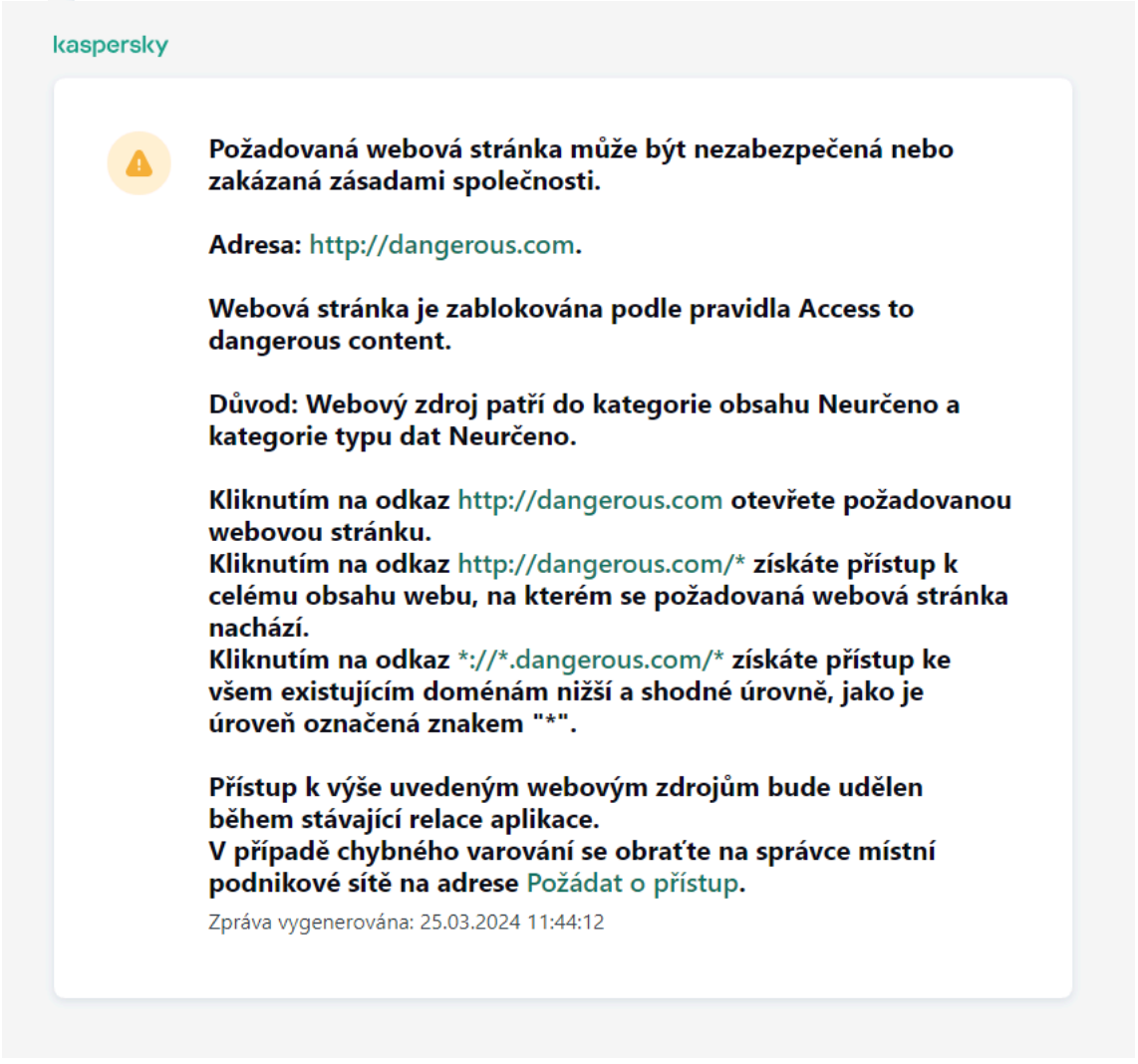
- Plán pravidel.

  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.

Ukončit aktivní uživatelské relace prohlížeče po uplatnění pravidla

Je-li toto políčko zaškrtnuto, součást Kontrola webu ukončí připojení k zablokovaným webovým zdrojům okamžitě po použití zásad. Prohlížeč okamžitě zastaví stahování dat z webové stránky. Když webovou stránku obnovíte nebo přejdete na jinou zakázanou webovou stránku, aplikace zobrazí varování.

Kontrola webu umožňuje okamžité odpojení webových zdrojů pouze ve webových prohlížečích. U jiných aplikací součást Kontrola webu omezuje pouze nová připojení.

Není-li toto políčko zaškrtnuto, omezuje Kontrola webu pouze nová připojení k zakázaným webovým zdrojům. Součást Kontrola webu neukončuje aktivní připojení.

Šablony

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. Šablona zprávy, kterou lze odeslat správci sítě LAN, pokud se uživatel domnívá, že k zablokování došlo omylem. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k webové stránce určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Pro správu šablon zprávy jsou k dispozici speciální proměnné (např. `%USER_NAME%`). Proměnné umožňují použití jedné šablony zprávy pro různé počítače.

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.

Prohlížeče podporující funkci monitorování: Microsoft Edge, Microsoft Internet Explorer, Google Chrome, Yandex Browser, Mozilla Firefox. Monitorování aktivity uživatele v jiných prohlížečích nefunguje.

Sledování aktivity uživatele na internetu může vyžadovat více prostředků počítače při dešifrování provozu HTTPS.

Kontrola zařízení

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.

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 **Advanced** → **Repositories** → **Hardware**.

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 – ⊘.
  - Podle pravidel (pouze tiskárny a přenosná zařízení) – .
  - V závislosti na sběrnici připojení (kromě 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). Pokud je u typu zařízení vybrán režim **V závislosti na sběrnici připojení**, aplikace povolí nebo zakáže přístup k zařízení v závislosti na rozhraní připojení (např. 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.

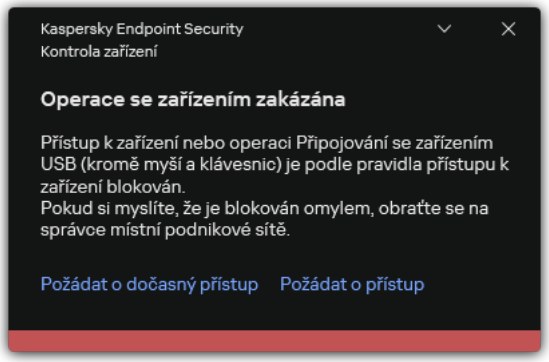
  - **Zařízení dle masky ID**. Pokud používáte více zařízení s podobnými ID, můžete je přidat do seznamu důvěryhodných zařízení pomocí masek. Znak `*` nahrazuje jakoukoli sadu znaků. Kaspersky Endpoint Security při zadávání masky znak `?`. Například `WDC_C*`.

  - **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.

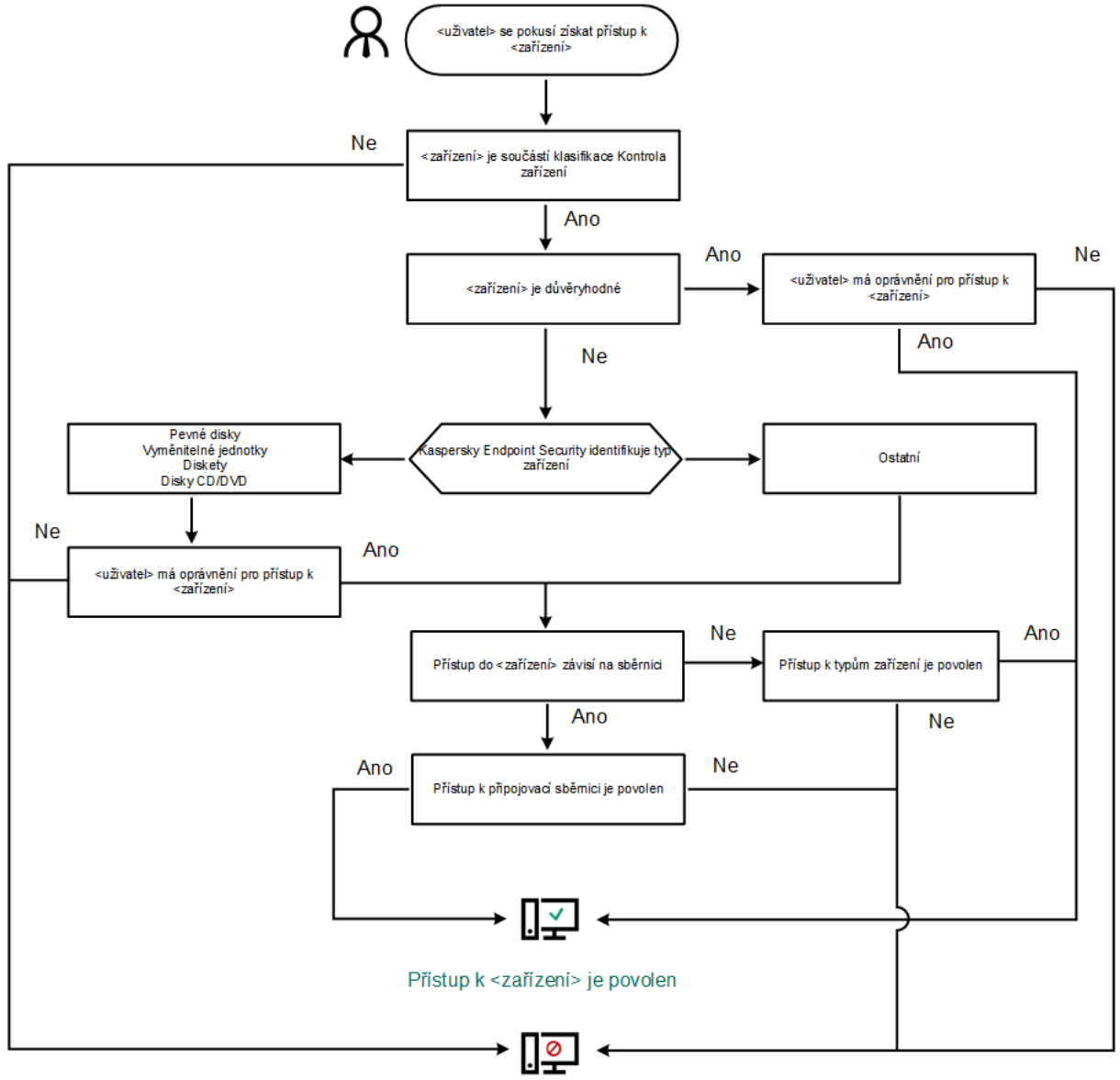
Když je k počítači připojeno zařízení, které je blokováno součástí Kontrola zařízení, aplikace Kaspersky Endpoint Security zablokuje přístup a zobrazí upozornění (viz obrázek níže).



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. Pomocí tohoto tlačítka 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. Pokud je vybrán režim **V závislosti na sběrnici připojení**, aplikace Kaspersky Endpoint Security povolí nebo odepře přístup k zařízením v závislosti na typu připojovací sběrnice.
Důvěryhodná zařízení	Seznam důvěryhodných zařízení a uživatelů, kterým byl udělen přístup k těmto zařízením.

Sloučit hodnoty při dědění *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Tím se sloučí 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 zařízení pro celou organizaci. Zděděné položky seznamu v podřízené zásadě nelze odstranit ani upravit. Položky v seznamu důvěryhodných zařízení, 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. Tato funkce také umožňuje slučování seznamů v profilech zásad. Chcete-li sloučit seznamy, povolte v profilu s nejvyšší prioritou dědění nastavení z profilu s nižší prioritou. Další informace o prioritách profilů zásad najdete v nápovědě k aplikaci Kaspersky Security Center.
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. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování přístupu k zařízení určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

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* nebo jiná kategorie), 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. Správce může vytvořit mnoho pravidel. Jedna aplikace může splňovat kritéria více pravidel. Priorita pravidla blokování je vyšší než priorita pravidla povolení. Kaspersky Endpoint Security při každém spuštění zkontroluje, zda aplikace splňuje pravidlo. Aplikace Kaspersky Endpoint Security postupně porovnává aplikaci se všemi pravidly součásti Kontrola aplikací.

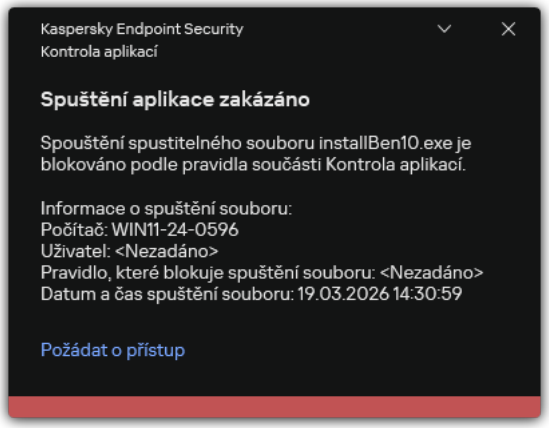
3. Volba režimu součásti Kontrola aplikací.

   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.

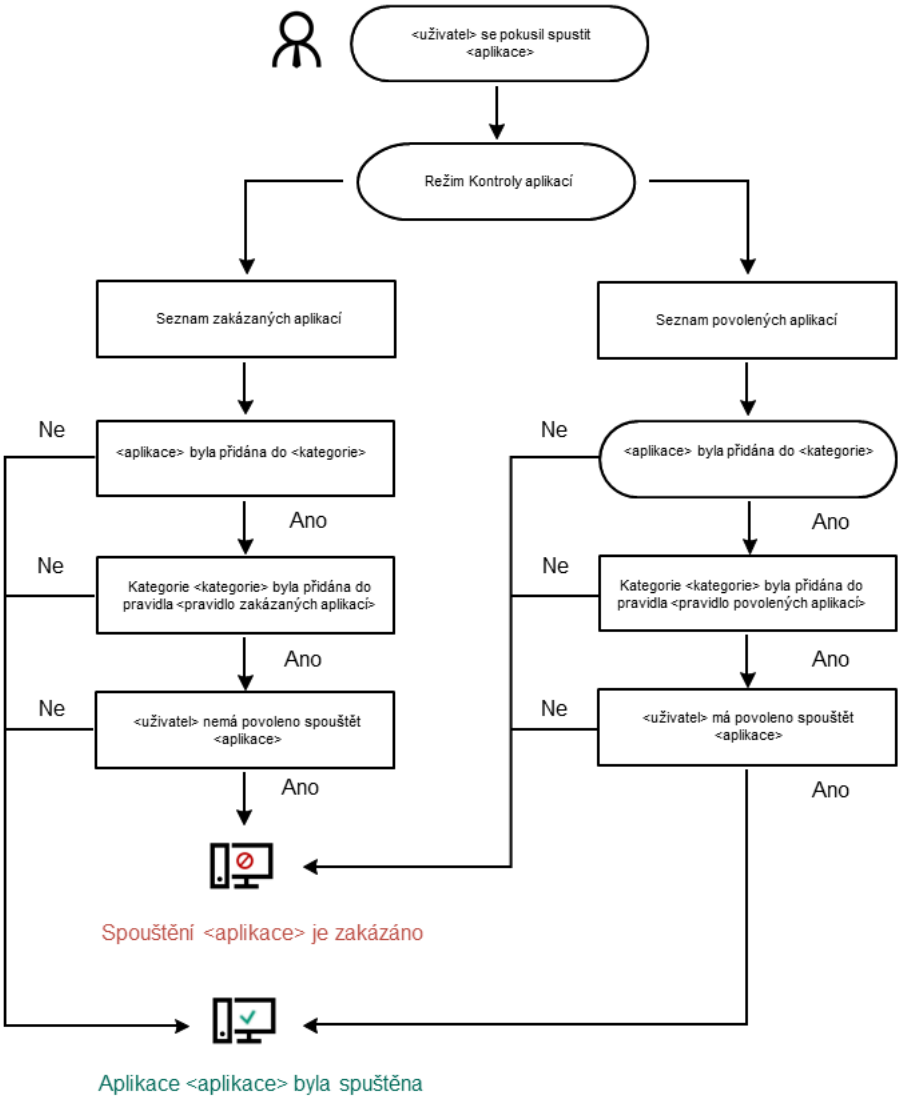
  Pravidla součásti Kontrola aplikací vytvořená v konzole pro správu aplikace Kaspersky Security Center jsou založena na vašich vlastních kategoriích aplikací, nikoli na podmínkách zahrnutí a vyloučení, jako je tomu v místním rozhraní aplikace Kaspersky Endpoint Security.

- 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
Akce při spuštění aplikací blokovaných pravidly	**Použít pravidla**. Kaspersky Endpoint Security řídí spouštění aplikací podle zvoleného režimu. **Otestovat pravidla**. Kaspersky Endpoint Security povolí spuštění aplikace, která je v aktuálním režimu součásti Kontrola aplikací zablokována, ale zaznamená informace o spuštění aplikace do zprávy protokolu.

Režim kontroly spouštění aplikací

Máte na výběr tyto možnosti:

- **Seznam blokovaných položek**. Pokud je vybrána tato možnost, umožní součást Kontrola aplikací všem uživatelům spouštět libovolnou aplikaci 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.

Monitorovat zavádění modulů 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 „**Golden Image\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.

Používat přísné ověřování digitálního podpisu

Jako aktivující podmínku pro pravidlo součásti Kontrola aplikací můžete vybrat certifikát.

Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané pouze pomocí certifikátů z úložiště důvěryhodných systémových certifikátů. Aplikace podepsané takovým certifikátem jsou také považovány za důvěryhodné součástmi ochrany, například úlohou *Kontrola malwaru*. Pokud však v pravidlu součásti Kontrola aplikací zadáte certifikát z jiného úložiště, aplikace Kaspersky Endpoint Security takové pravidlo nepoužije.

Není-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security použije pravidla na aplikace podepsané certifikátem z úložiště důvěryhodných kořenových certifikátů systému Windows. Takové aplikace nejsou součástí důvěryhodné zóny. Součásti ochrany monitorují aktivitu těchto aplikací.

Šablony zpráv o blokování aplikace

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. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování spuštění aplikace určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Adaptivní kontrola anomálií

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 netypického 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 **Rule triggers in Smart Training state**.

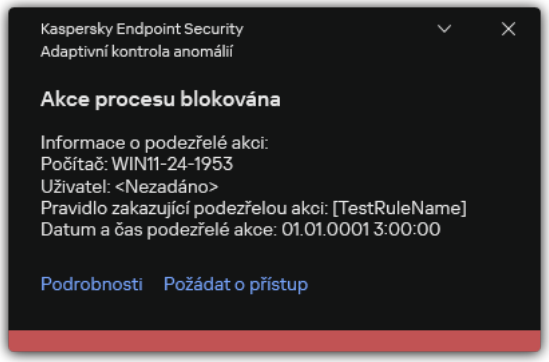
2. Analýza zprávy o aktivaci pravidel.

   Správce analyzuje zprávu o aktivaci pravidel nebo obsah úložiště **Rule triggers in Smart Training state**. 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 se konfiguruje v reálném čase 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 **Rule triggers in Smart Training state**. Doporučujeme přečíst si zprávu o aktivaci pravidel a obsahu úložiště **Rule triggers in Smart Training state**.

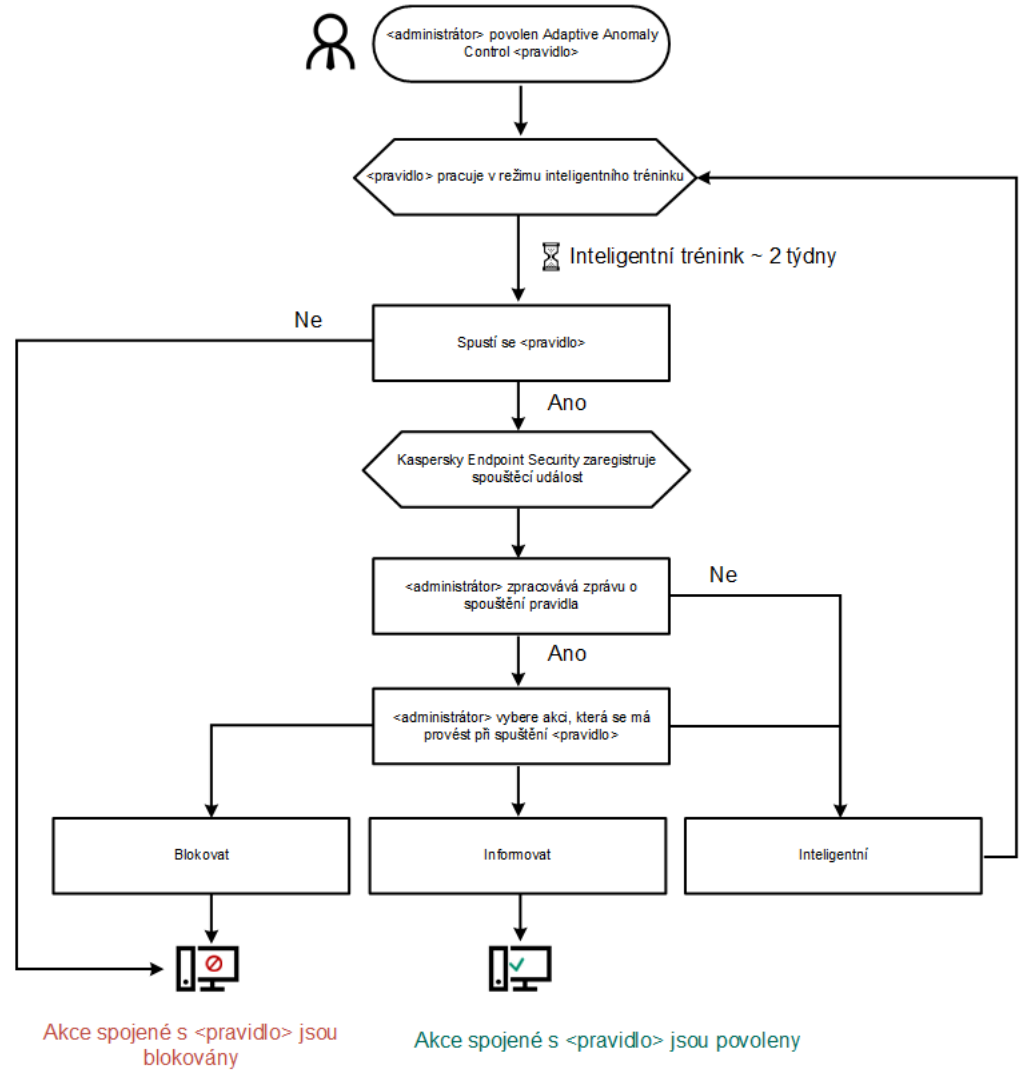
Pokud se škodlivá aplikace pokusí provést akci, aplikace Kaspersky Endpoint Security akci zablokuje a zobrazí upozornění (viz obrázek níže).



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 součásti Adaptivní kontrola anomálií *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Tato zpráva obsahuje informace o stavu detekčních pravidel součásti Adaptivní kontrola anomálií (například *Zakázáno* nebo *Blokovat*). Zpráva je generována pro všechny skupiny pro správu.
Zpráva o aktivovaných pravidlech součásti Adaptivní kontrola anomálií *(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 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. Poté, co uživatel požádá o poskytnutí přístupu, Kaspersky Endpoint Security odešle událost do aplikace Kaspersky Security Center: **Zpráva o blokování aktivity aplikace určená pro správce**. Popis události obsahuje zprávu správci s nahrazenými proměnnými. Tyto události můžete zobrazit v konzole aplikace Kaspersky Security Center pomocí předdefinovaného výběru událostí **User requests**. Pokud vaše organizace nemá nasazenou aplikaci Kaspersky Security Center nebo není k dispozici připojení k serveru pro správu, aplikace odešle zprávu správci na zadanou e-mailovou adresu.

Monitorování integrity systému

Tato součást je dostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro servery. Tato součást je nedostupná, pokud je aplikace Kaspersky Endpoint Security nainstalovaná v počítači se systémem Windows pro pracovní stanice.

Od verze 12.6 obsahuje aplikace Kaspersky Endpoint Security pro systém Windows místo součásti Monitor integrity souborů součást Monitorování integrity systému. Součást Monitorování integrity systému zahrnuje veškeré funkce součásti Monitor integrity souborů a navíc umožňuje sledovat změny registru a připojení externích zařízení.

Součást Monitorování integrity systému monitoruje změny v operačním systému, které mohou naznačovat narušení zabezpečení počítače. V případě zjištění takovýchto změn Kaspersky Endpoint Security vygeneruje odpovídající události a upozorní správce. Monitorování integrity systému může fungovat v reálném čase a může také provádět kontroly integrity systému na vyžádání.

Monitorování integrity systému v reálném čase

V režimu monitorování v reálném čase Monitorování integrity systému sleduje změny v objektech, které jste zahrnuli do rozsahu součásti (*rozsah monitorování*). Monitorování integrity systému také umožňuje blokovat neoprávněný přístup k takovým objektům v reálném čase.

Kontrola integrity systému na vyžádání

Kontrola integrity systému na vyžádání je úloha, kterou můžete spustit ručně nebo podle plánu. Chcete-li úlohu *Kontrola integrity systému* spustit, musíte nakonfigurovat rozsah součásti (*rozsah sledování*) a vytvořit základní stav. *Základní stav* je zaznamenaný stav objektů v systému, který aplikace používá jako referenci při porovnávání s aktuálním stavem.

Nastavení součásti Monitorování integrity systému

Parametr	Popis
Režim fungování pro pravidla blokování	• **Blokovat**. V tomto režimu blokuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost. • **Informovat**. V tomto režimu umožňuje součást Monitorování integrity systému akce se soubory a klíči registru z rozsahu monitorování a vygeneruje příslušnou událost.
Monitorování integrity systému v reálném čase	V režimu monitorování v reálném čase Monitorování integrity systému sleduje změny v objektech, které jste zahrnuli do rozsahu součásti (*rozsah monitorování*). Monitorování integrity systému také umožňuje blokovat neoprávněný přístup k takovým objektům v reálném čase.
Monitorovat zařízení	Monitorování integrity systému monitoruje připojení a odpojení externích zařízení.
Monitorovat soubory a registr	Monitorování integrity systému monitoruje změny souborů, složek a registru.
Kontrola integrity systému	Kontrola integrity systému na vyžádání je úloha, kterou můžete spustit ručně nebo podle plánu. Chcete-li úlohu *Kontrola integrity systému* spustit, musíte nakonfigurovat rozsah součásti (*rozsah sledování*) a vytvořit základní stav. *Základní stav* je zaznamenaný stav objektů v systému, který aplikace používá jako referenci při porovnávání s aktuálním stavem.

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 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. Kaspersky Anti Targeted Attack Platform obsahuje tři funkční jednotky:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Všechny funkční jednotky nebo jednotlivé funkční jednotky můžete zakoupit samostatně. Podrobnosti o tomto 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 nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

Sandbox

Aplikace Kaspersky Endpoint Security pro systém Windows obsahuje integrovaného agenta pro integraci s řešením Kaspersky Sandbox. Součást *Sandbox* detekuje a automaticky blokuje pokročilé hrozby na počítačích. Součást Sandbox analyzuje chování objektu, aby detekovala škodlivou aktivitu a aktivitu charakteristickou pro cílené útoky na IT infrastrukturu organizace. Sandbox analyzuje a kontroluje objekty na speciálních serverech s nasazenými virtuálními bitovými kopiemi operačních systémů Microsoft Windows (servery Sandbox). Podrobnosti o tomto řešení najdete v nápovědě k součásti Kaspersky Sandbox a nápovědě k řešení Kaspersky Anti Targeted Attack Platform.

Počínaje verzí 12.7 podporuje aplikace Kaspersky Endpoint Security pro systém Windows součást Sandbox, která je součástí řešení Kaspersky Anti Targeted Attack Platform. Na rozdíl od řešení Kaspersky Sandbox umožňuje součást KATA Sandbox kontrolovat soubory nejen automaticky, ale i ručně z místní nabídky souboru.

KATA Sandbox vyžaduje nasazení aplikace Kaspersky Anti Targeted Attack Platform 7.0 nebo novější.

Součást lze spravovat pouze pomocí webové konzoly Kaspersky Security Center. Tuto součást nemůžete spravovat pomocí konzoly pro správu (MMC).

Nastavení součásti Sandbox

Parametr	Popis
Integration mode	**Kaspersky Sandbox**. Integrace s řešením Kaspersky Sandbox. Aplikace odesílá soubory ke kontrole do součásti Kaspersky Sandbox pouze v automatickém režimu. **KATA Sandbox**. Integrace se součástí Sandbox řešení Kaspersky Anti Targeted Attack Platform. Můžete vybrat režim odeslání souborů ke kontrole: • **Manually**. Uživatel ručně odešle soubor ke kontrole z kontextové nabídky (**Odesílat do řešení Sandbox**). • **Automatically**. Aplikace automaticky detekuje objekty a odesílá je do součásti Sandbox ke kontrole. • **Combined**.
Server connection settings	**Timeout (msec)**. Vypršel časový limit připojení pro Sandbox (u Kaspersky Sandbox) nebo server Central Node (u KATA). Po uplynutí nastaveného časového limitu odešle aplikace Kaspersky Endpoint Security požadavek na další server. Pokud je rychlost připojení nízká nebo je připojení nestabilní, můžete prodloužit časový limit připojení pro server. Doporučovaný časový limit požadavku je 0,5 sekundy a méně.

	Request queue. Velikost složky fronty žádostí. Při odesílání více objektů ke kontrole v součásti Sandbox vytvoří Kaspersky Endpoint Security frontu požadavků. Ve výchozím nastavení je velikost složky fronty žádostí omezena na 100 MB. Jakmile je dosaženo maximální velikosti, Sandbox přestane přidávat nové žádosti do fronty a odešle odpovídající událost do aplikace Kaspersky Security Center. Velikost složky fronty žádostí můžete konfigurovat v závislosti na konfiguraci serveru. **Server TLS certificate**. Chcete-li nakonfigurovat důvěryhodné připojení se serverem Sandbox (u Kaspersky Sandbox) nebo serverem Central Node (u KATA), musíte si připravit certifikát TLS. Poté musíte přidat certifikát do počítače pomocí zásady. Certifikát musíte také přidat na server Sandbox (u Kaspersky Sandbox) nebo na server Central Node (u KATA). **Use two-way authentication** (pouze pro KATA Sandbox). Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.
Connection to Sandbox servers	**Kaspersky Sandbox**. Nastavení připojení k serveru Sandbox. Servery používají ke spouštění objektů, které je třeba kontrolovat nasazené bitové kopie operačních systémů Microsoft Windows. Můžete zadat IP adresu (IPv4 nebo IPv6) nebo plně kvalifikovaný název domény. **KATA Sandbox**. Nastavení připojení k serveru součásti Central Node. Central Node vybírá optimální nastavení kontroly a vyrovnává zátěž mezi servery Sandbox.
Action on threat detection	**Move copy to Quarantine, delete object**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security odstraní škodlivý objekt nalezený v počítači. Před odstraněním objektu vytvoří aplikace Kaspersky Endpoint Security záložní kopii pro případ, že bude nutné objekt později obnovit. Kaspersky Endpoint Security přesune záložní kopii do karantény. **Run Critical Areas Scan**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security spustí úlohu *Kontrola kritických oblastí*. Ve výchozím nastavení aplikace Kaspersky Endpoint Security kontroluje paměť jádra, spuštěné procesy a spouštěcí sektory disků. **Create IOC Scan task**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security automaticky vytvoří úlohu *Kontrola IOC (autonomní úloha kontroly IOC)*. Pro tuto úlohu můžete nakonfigurovat režim spuštění, rozsah kontroly a akci při detekci IOC: odstranit objekt, spustit úlohu *Kontrola kritických oblastí*. Chcete-li upravit další nastavení úlohy *Kontrola IOC*, přejděte do nastavení úlohy.
IOC Scan scope	**Critical file areas**. Pokud je vybrána tato možnost, aplikace Kaspersky Endpoint Security provede kontrolu IOC pouze v kritických oblastech souboru počítače: paměti jádra a spouštěcí sektory. **File areas on system drives of the computer**. Je-li vybrána tato možnost, provede Kaspersky Endpoint Security kontrolu IOC na systémové jednotce počítače.
Run IOC Scan task	**Manually**. Režim spuštění, ve kterém můžete úlohu *Kontrola IOC* spustit ručně v době, kdy je to pro vás výhodné. **Automatically**. Režim spuštění, ve kterém aplikace Kaspersky Endpoint Security spouští úlohu *Kontrola IOC* automaticky, kdykoli je detekována hrozba. **Run only when the computer is idle**. Režim spuštění, ve kterém aplikace Kaspersky Endpoint Security spouští úlohu *Kontrola IOC*, když je aktivní spořič obrazovky nebo je obrazovka zamčená. Pokud uživatel odemkne počítač, aplikace Kaspersky Endpoint Security úlohu pozastaví. To znamená, že dokončení úlohy může trvat několik dní.

Managed Detection and Response

Kaspersky Endpoint Security pro systém Windows podporuje integraci s řešením Managed Detection and Response. Řešení *Kaspersky Managed Detection and Response (MDR)* automaticky detekuje a analyzuje bezpečnostní incidenty ve vaší infrastruktuře. K tomu používá MDR telemetrická data přijatá z koncových bodů a strojové učení. MDR zasílá údaje o incidentech odborníkům společnosti Kaspersky. Tito odborníci pak mohou incident zpracovat a například přidat nový záznam do antivirových databází. Alternativně mohou odborníci vydat doporučení ke zpracování incidentu a například navrhnout izolaci počítače od sítě. Podrobné informace o tom, jak řešení funguje, najdete v nápovědě k aplikaci Kaspersky Managed Detection and Response .

Nastavení součásti Managed Detection and Response

Parametr	Popis
Konfigurační soubor MDR	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 nápovědě k řešení Kaspersky Managed Detection and Response .

Endpoint Detection and Response

Aplikace Kaspersky Endpoint Security pro systém Windows obsahuje integrovaného agenta pro řešení Kaspersky Endpoint Detection and Response Optimum (dále také „EDR Optimum"). Počínaje verzí 11.8.0 obsahuje aplikace Kaspersky Endpoint Security pro systém Windows integrovaného agenta pro řešení Kaspersky Endpoint Detection and Response Expert (dále také „EDR Expert"). *Kaspersky Endpoint Detection and Response* je řada řešení pro ochranu podnikové IT infrastruktury před pokročilými kybernetickými hrozbami. Funkce řešení kombinuje automatickou detekci hrozeb se schopností reagovat na tyto hrozby a čelit tak pokročilým útokům včetně nových exploitů, ransomwaru, bezsouborových útoků a metod využívajících legitimní systémové nástroje. EDR Expert nabízí více funkcí sledování hrozeb a reakce na ně než EDR Optimum. Podrobnosti o těchto řešeních najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert .

Kaspersky Endpoint Detection and Response kontroluje a analyzuje vývoj hrozeb a poskytuje *bezpečnostním pracovníkům* nebo *správci* informace o potenciálním útoku, které jsou nezbytné pro včasnou reakci. Kaspersky Endpoint Detection and Response zobrazí podrobnosti o výstraze v samostatném okně. *Upozornění* je událost v podnikové IT infrastruktuře, kterou aplikace identifikovala jako neobvyklou nebo podezřelou a která může představovat bezpečnostní hrozbu pro podnikovou IT infrastrukturu. *Podrobnosti o výsledcích detekce* je nástroj pro prohlížení všech shromážděných informací o detekované hrozbě. Mezi výsledky detekce patří například historie souborů objevujících se v počítači. Podrobnosti o správě podrobností o výsledcích detekce najdete v nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert.

Součást EDR Optimum můžete nakonfigurovat ve webové konzole a v cloudové konzole. Nastavení součásti pro nástroj EDR Expert je k dispozici pouze v cloudové konzole.

Nastavení součásti Endpoint Detection and Response

Parametr	Popis
Enable advanced system activity logging	Rozšířená telemetrie zlepšuje přesnost zjišťování IOC, ale využívá více prostředků počítače. Pro retrospektivní kontrolu IOC doporučujeme v počítači povolit rozšířenou telemetrii. *Retrospektivní kontrola IOC* je režim úlohy *IOC Scan*, ve kterém aplikace Kaspersky Endpoint Security kontroluje indikátory narušení pomocí dat za určité časové období. Tento režim je určen pro hledání indikátorů narušení podle telemetrie chráněného počítače, jako je síťová aktivita, procesy, soubory a jiná telemetrie. Je-li rozšířená telemetrie zakázána, Kaspersky Endpoint Security může střídat informace o zjištěných indikátorech narušení.
Network Isolation	Automatická izolace počítače od sítě v reakci na zjištěné hrozby. Když je izolace sítě zapnutá, aplikace přeruší všechna aktivní připojení a zablokuje všechna nová připojení TCP/IP v počítači. Aplikace ponechává aktivní pouze následující připojení: • Připojení uvedená v části Výjimky z izolace sítě. • Připojení iniciovaná službami Kaspersky Endpoint Security. • Připojení iniciovaná součástí Kaspersky Security Center Network Agent.
Automatically unlock isolated device in (hours)	Izolaci sítě lze vypnout automaticky po určené době nebo ručně. Ve výchozím nastavení aplikace Kaspersky Endpoint Security vypne izolaci sítě 5 hodin po zahájení izolace.
Network isolation exclusions	Seznam pravidel pro výjimky z izolace sítě. Síťová připojení, která odpovídají pravidlům, nejsou na počítačích blokována, když je zapnutá izolace sítě. Chcete-li nakonfigurovat výjimky z izolace sítě, můžete použít seznam *standardních síťových profilů*. Ve výchozím nastavení zahrnují výjimky síťové profily obsahující pravidla, která zajišťují nepřetržitý provoz zařízení s rolemi serveru DNS/DHCP a klienta DNS/DHCP. Můžete rovněž upravit nastavení standardních síťových profilů nebo výjimky definovat ručně. Výjimky uvedené ve vlastnostech zásad se použijí pouze v případě, že je izolace sítě automaticky zapnuta v reakci na zjištěnou hrozbu. Výjimky uvedené ve vlastnostech počítače se použijí pouze v případě, že je ve vlastnostech počítače v konzole Kaspersky Security Center nebo v podrobnostech o výstraze ručně zapnuta izolace sítě.
Execution Prevention	Ovládejte spouštění spustitelných souborů a skriptů a otevírání souborů ve formátu aplikací Office. Můžete například zabránit spouštění aplikací, které jsou na vybraném počítači považovány za nezabezpečené. Prevence spouštění podporuje sadu přípon kancelářských souborů a sadu interpretů skriptů. Chcete-li použít součást Prevence spouštění, musíte přidat pravidla prevence spouštění. *Pravidlo prevence spouštění* je sada kritérií, která aplikace bere v úvahu při reakci na spuštění objektu, například při blokování spuštění objektu. Aplikace identifikuje soubory podle jejich cest nebo kontrolních součtů vypočítaných pomocí algoritmů hash MD5 a SHA256.
Action on execution or opening of forbidden object	**Block and add to event log**. V tomto režimu aplikace blokuje spouštění objektů nebo otevírání dokumentů, které odpovídají kritériím pravidla prevence. Aplikace také publikuje událost o pokusech o spuštění objektů nebo otevření dokumentů do protokolu událostí systému Windows a protokolu událostí aplikace Kaspersky Security Center. **Add to event log**. V tomto režimu aplikace Kaspersky Endpoint Security publikuje událost o pokusech o spuštění spustitelných objektů nebo otevřených dokumentech, které odpovídají kritériím pravidel prevence do protokolu událostí systému Windows a Kaspersky Security Center, ale neblokuje pokus o spuštění nebo otevření objektu nebo dokumentu. Tento režim je ve výchozím nastavení vybrán.
Execution prevention rules	*Pravidlo prevence spouštění* je sada kritérií, která aplikace bere v úvahu při reakci na spuštění objektu, například při blokování spuštění objektu. Aplikace identifikuje soubory podle jejich cest nebo kontrolních součtů vypočítaných pomocí algoritmů hash MD5 a SHA256.

Cloud Sandbox	*Cloud Sandbox* je technologie, která vám umožňuje v počítači detekovat pokročilé hrozby. Kaspersky Endpoint Security automaticky předává zjištěné soubory do Cloud Sandboxu na analýzu. Cloud Sandbox tyto soubory spustí v izolovaném prostředí, aby zjistil škodlivou aktivitu, a rozhodne o jejich reputaci. Údaje o těchto souborech jsou poté odeslány do služby Kaspersky Security Network. Pokud Cloud Sandbox zjistí škodlivý soubor, aplikace Kaspersky Endpoint Security provede příslušnou akci, aby tuto hrozbu eliminovala ve všech počítačích, kde je tento soubor zjištěn. Technologie Cloud Sandbox je trvale povolena a je k dispozici všem uživatelům služby Kaspersky Security Network bez ohledu na typ licence, který používají. Pokud je toto políčko zaškrtnuté, aplikace Kaspersky Endpoint Security povolí počítadlo u hrozeb zjištěných pomocí technologie Cloud Sandbox v hlavním okně aplikace v části **Technologie detekce hrozeb**. Aplikace Kaspersky Endpoint Security bude technologii detekce hrozeb Cloud Sandbox uvádět také v událostech aplikací a v části *Report on threats* v konzole aplikace Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premise)

Endpoint Detection and Response Expert (on-premise)

Kaspersky Endpoint Security pro systém Windows podporuje integraci s řešením Managed Detection and Response Expert (on-premise). *Kaspersky Endpoint Detection and Response Expert (on-premise)* je podnikové řešení kybernetické bezpečnosti zahrnující aplikace společnosti Kaspersky, které umožňují organizaci bránit se před většinou typů kybernetických rizik a pokrývají nejdůležitější scénáře šíření hrozeb. Součásti EDR Expert (on-premise) jsou nasazeny na otevřené platformě OSMP (Open Single Management Platform). Tato platforma spouští scénáře pro různé platformy v jediném rozhraní a umožňuje integrovat aplikace Kaspersky s aplikacemi třetích stran do komplexního systému zabezpečení.

Jedním z ústředních prvků řešení je *SIEM*. SIEM sleduje události pocházející ze všech součástí a uvádí tyto události do vzájemného vztahu pomocí pravidel definovaných dodavatelem a uživatelem. EDR Expert (on-premise) se dívá na protokoly a telemetrii přijaté z podnikové infrastruktury za účelem automatického zjišťování útoků a umožňuje vyšetřovat incidenty pomocí jednotného grafu vyšetřování, který kombinuje všechny události shromážděné v aplikaci EDR Expert (on-premise), včetně událostí z aplikací společnosti Kaspersky a produkty pro zabezpečení informací třetích stran.

Pro reakci na pokročilé incidenty používá EDR Expert (on-premise) přednastavené a uživatelem definované scénáře. Můžete také použít akce odezvy z aplikací třetích stran a scénáře reakce, které zahrnují více aplikací.

Endpoint Detection and Response (KATA)

Aplikace Kaspersky Endpoint Security pro systém Windows podporuje fungování se součástí Kaspersky Endpoint Detection and Response jako součásti řešení Kaspersky Anti Targeted Attack Platform (EDR (KATA)). 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. Kaspersky Anti Targeted Attack Platform obsahuje tři funkční jednotky:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Všechny funkční jednotky nebo jednotlivé funkční jednotky můžete zakoupit samostatně. Podrobnosti o tomto řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

Aplikace Kaspersky Endpoint Security se instaluje na jednotlivé počítače v podnikové IT infrastruktuře a nepřetržitě sleduje procesy, otevřená síťová připojení a upravované soubory. Informace o událostech v počítači (telemetrická data) jsou odesílány na server Kaspersky Anti Targeted Attack Platform. V tomto případě aplikace Kaspersky Endpoint Security také odešle na server Kaspersky Anti Targeted Attack Platform informace o hrozbách objevených aplikací a také informace o výsledcích zpracování těchto hrozeb.

Integrace EDR (KATA) a NDR (KATA) se konfiguruje v konzole aplikace Kaspersky Security Center. Integrovaný agent je pak spravován pomocí konzoly Kaspersky Anti Targeted Attack Platform, včetně spouštění úloh, správy objektů v karanténě, prohlížení zpráv a dalších akcí.

Nastavení řešení Endpoint Detection and Response Expert (on-premise)

Parametr	Popis
Connection to telemetry collection servers	*Server pro shromažďování telemetrie* je server, který je součástí řešení SIEM, které shromažďuje, normalizuje, uvádí do vzájemného vztahu, analyzuje a ukládá informace o událostech, k nimž dochází v počítači. Chcete-li se připojit k serverům pro sběr telemetrie (KUMA), nakonfigurujte následující položky: • **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru. • **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). • **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem.

Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

Address a **Port** (servery pro sběr telemetrie)

Nastavení pro připojování k serverům pro shromažďování telemetrie. Můžete zadat IP adresu (IPv4 nebo IPv6).

Můžete přidat více adres serveru pro shromažďování telemetrie. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.

Send telemetry to telemetry collection servers

Tato funkce umožňuje zcela vypnout odesílání telemetrických údajů na server KATA. Pokud například používáte Kaspersky Anti Targeted Attack Platform spolu s jiným řešením, které také využívá telemetrii, můžete odesílání telemetrie pro KATA (EDR) vypnout. To vám umožní optimalizovat zatížení serveru pro tato řešení. Pokud máte nasazené řešení Managed Detection and Response a součást KATA (EDR), můžete použít telemetrii MDR a vytvářet úlohy Reakce na hrozby v KATA (EDR).

- **Send telemetry with IOA only**. To umožňuje optimalizaci telemetrie a odesílání telemetrie pouze pomocí IOA. *Indikátor útoku (IOA)* je pravidlo, které obsahuje popis podezřelého chování v systému, které může naznačovat cílený útok. Aplikace porovnává průběžné chování v systému s těmito pravidly a zaprotokoluje události, které ukazují na cílený útok. Aplikace používá technologii *kontrola streamování*, která umožňuje sledování těchto událostí v reálném čase.
- **Maximum event transmission delay (sec)**. Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
- **Limit the number of event packets per transmission**. Aplikace se synchronizuje se serverem, když se vyrovnávací paměť zaplní událostmi. Výchozí hodnota je 1024 událostí. Tato funkce umožňuje zakázat ukládání událostí do vyrovnávací paměti před synchronizací se serverem.

Enable request throttling

Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.

Konfigurace nastavení telemetrie:

- **Maximum number of events per hour**. Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
- **Percentage of event limit excess**. Aplikace třídí události podle typu (například události „změny registru“) a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.

Send sync request to server every (min)

Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.

Connection to response servers

Odpovědní server je server pro příjem a kontrolu dat, studium chování objektů a publikování výsledků těchto studií.

Nakonfigurujte následující připojení k odpovědním serverům:

- **Timeout (sec)**. Maximální časový limit odpovědi serveru. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru.
- **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem. Certifikát TLS můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)).
- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat na otevřené platformě OSMP (Open Single Management Platform) (viz pokyny v nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise)). Po konfiguraci nastavení serveru musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

Address a **Port** (odpovědní servery)

Nastavení pro připojování k odpovědním serverům. Můžete zadat IP adresu (IPv4 nebo IPv6).

Můžete přidat více adres serveru pro shromažďování telemetrie. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.

Nastavení součásti Endpoint Detection and Response (KATA)

Parametr	Popis

Send sync request to server every (min)

Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.

Connection to KATA servers

Nakonfigurujte následující připojení k serveru Central Node:

- **Timeout (sec)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node.
- **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform).
- **Use two-way authentication**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

  Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

Address a **Port** (servery KATA)

Nastavení připojení k serverům platformy Kaspersky Anti Targeted Attack Platform. Zadejte IP adresu (IPv4 nebo IPv6) a port serveru Central Node, k němuž se chcete připojovat.

Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru pomocí první IP adresy. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit pomocí druhé IP adresy v seznamu a tak dále.

Send telemetry to KATA

Tato funkce umožňuje zcela vypnout odesílání telemetrických údajů na server KATA. Pokud například používáte Kaspersky Anti Targeted Attack Platform spolu s jiným řešením, které také využívá telemetrii, můžete odesílání telemetrie pro KATA (EDR) vypnout. To vám umožní optimalizovat zatížení serveru pro tato řešení. Pokud máte nasazené řešení Managed Detection and Response a součást KATA (EDR), můžete použít telemetrii MDR a vytvářet úlohy Reakce na hrozby v KATA (EDR).

Konfigurace nastavení telemetrie:

- **Maximum event transmission delay (sec)**. Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
- **Maximum number of event packages**. Aplikace se synchronizuje se serverem, když se vyrovnávací paměť zaplní událostmi. Výchozí hodnota je 1024 událostí.

Enable request throttling

Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.

Konfigurace nastavení telemetrie:

- **Maximum number of events per hour**. Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
- **Percentage of event limit excess**. Aplikace třídí události podle typu (například události „změny registru“) a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.

Network Detection and Response (KATA)

Aplikace Kaspersky Endpoint Security pro systém Windows podporuje fungování se součástí Kaspersky Network Detection and Response jako součásti řešení Kaspersky Anti Targeted Attack Platform (EDR (KATA)). 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. Kaspersky Anti Targeted Attack Platform obsahuje tři funkční jednotky:

- Kaspersky Anti Targeted Attack Platform (*KATA*)
- Kaspersky Endpoint Detection and Response (*EDR (KATA)*)
- Network Detection and Response (*NDR (KATA)*)

Všechny funkční jednotky nebo jednotlivé funkční jednotky můžete zakoupit samostatně. Podrobnosti o tomto řešení najdete v nápovědě k platformě Kaspersky Anti Targeted Attack Platform.

Aplikace Kaspersky Endpoint Security se instaluje na jednotlivé počítače v podnikové IT infrastruktuře a nepřetržitě sleduje procesy, otevřená síťová připojení a upravované soubory. Informace o událostech v počítači (telemetrická data) jsou odesílány na server Kaspersky Anti Targeted Attack Platform. V tomto případě aplikace Kaspersky Endpoint Security také odešle na server Kaspersky Anti Targeted Attack Platform informace o hrozbách objevených aplikací a také informace o výsledcích zpracování těchto hrozeb.

Integrace EDR (KATA) a NDR (KATA) se konfiguruje v konzole aplikace Kaspersky Security Center. Integrovaný agent je pak spravován pomocí konzoly Kaspersky Anti Targeted Attack Platform, včetně spouštění úloh, správy objektů v karanténě, prohlížení zpráv a dalších akcí.

Parametry Network Detection and Response (KATA)

Parametr	Popis
Nastavení připojení k serveru	**Doba vypršení časového limitu (s)**. Maximální časový limit odpovědi serveru Central Node. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru Central Node. **Certifikát TLS serveru**. Certifikát TLS pro navázání důvěryhodného spojení se serverem Central Node. Certifikát TLS můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). **Používat ověřování na obou stranách**. Ověření na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a serverem Central Node. Chcete-li používat ověřování na obou stranách, musíte je povolit v nastavení serveru Central Node, poté si pořídit kryptokontejner a nastavit heslo pro jeho ochranu. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Kryptokontejner můžete získat v konzole součásti Kaspersky Anti Targeted Attack Platform (viz pokyny v nápovědě k součásti Kaspersky Anti Targeted Attack Platform). Po konfiguraci nastavení součásti Central Node musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem. Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.
Adresa a **Port**	Nastavení připojení k serverům platformy Kaspersky Anti Targeted Attack Platform. Zadejte IP adresu (IPv4 nebo IPv6) a port serveru Central Node, k němuž se chcete připojovat. Můžete přidat více adres serveru centrálního uzlu. Kaspersky Endpoint Security se pokusí o připojení k serveru na první IP adrese. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit k druhé IP adrese v seznamu a tak dále.
Odesílat požadavek na synchronizaci na server NDR každých (min.)	Frekvence požadavků na synchronizaci odesílaných na server. Během synchronizace Kaspersky Endpoint Security odesílá informace o změněných nastaveních aplikací a úlohách.
Maximální prodleva přenosu událostí (sek.)	Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
Povolit omezování požadavků	Tato funkce pomáhá optimalizovat zátěž serveru. Pokud je políčko zaškrtnuto, aplikace omezí přenášené události. Pokud počet událostí překročí nakonfigurované limity, aplikace Kaspersky Endpoint Security přestane odesílat události.
Maximální počet událostí za hodinu	Aplikace analyzuje tok telemetrických dat a omezí odesílání událostí, pokud tok událostí překročí nakonfigurovaný limit událostí za hodinu. Kaspersky Endpoint Security obnoví odesílání událostí po hodině. Výchozí nastavení je 3000 událostí za hodinu. Pokud je aplikace nainstalována na serveru, je datový tok telemetrie vyšší. U serverů se doporučuje zvýšit hodnotu na 60 000 událostí za hodinu.
Procentní hodnota překročení limitu událostí	Aplikace třídí události podle typu (například události „změny registru“) a omezuje přenos událostí, pokud poměr událostí stejného typu k celkovému počtu událostí překročí nakonfigurovaný limit v procentech. Kaspersky Endpoint Security obnoví odesílání událostí, když poměr ostatních událostí k celkovému počtu událostí bude opět dostatečně velký. Výchozí nastavení je 15 %.

Integrace s KUMA

Aplikace Kaspersky Endpoint Security pro systém Windows podporuje řešení Kaspersky Unified Monitoring and Analysis Platform. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* je řešení pro správu bezpečnostních informací a událostí (SIEM) pro IT infrastrukturu organizací. KUMA umožňuje detekovat, analyzovat a zmírňovat bezpečnostní hrozby dříve, než mohou způsobit škodu.

Nastavení integrace KUMA

Parametr	Popis
Maximum delay when sending events (sec)	Aplikace se synchronizuje se serverem a odesílá události po uplynutí intervalu synchronizace. Výchozí hodnota je 30 sekund.
Connection to KUMA servers	**Timeout (sec)**. Maximální časový limit odpovědi serveru KUMA. Když časový limit vyprší, Kaspersky Endpoint Security se pokusí připojit k jinému serveru KUMA. **Server certificate**. Certifikát TLS pro navázání důvěryhodného spojení se serverem KUMA. Certifikát TLS můžete získat v konzole Kaspersky Unified Monitoring and Analysis Platform (viz pokyny v řešení Kaspersky Unified Monitoring and Analysis Platform).

Chcete-li vytvořit důvěryhodné připojení, v konzole KUMA v nastavení konektoru TCP musíte vybrat režim TLS **With verification** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform).

Use two-way authentication. Ověřování na obou stranách při navazování zabezpečeného připojení mezi aplikací Kaspersky Endpoint Security a součástí KUMA. Chcete-li použít ověřování na obou stranách, musíte v konzole KUMA v nastavení konektoru tcp vybrat režim TLS **Custom PFX** (viz nastavení konektoru typu tcp v nápovědě k platformě Kaspersky Unified Monitoring and Analysis Platform). Poté musíte získat kryptokontejner a nastavit heslo pro ochranu kryptokontejneru. *Kryptokontejner* je PFX archiv s certifikátem a soukromým klíčem. Po konfiguraci nastavení součásti KUMA musíte také povolit obousměrné ověřování v nastavení aplikace Kaspersky Endpoint Security a načíst šifrovací kontejner chráněný heslem.

Kryptokontejner musí být chráněn heslem. Není možné přidat kryptokontejner s prázdným heslem.

Servery KUMA

Připojení k serverům Kaspersky Unified Monitoring and Analysis Platform. Můžete zadat IP adresu (IPv4 nebo IPv6).

Můžete přidat více adres serveru KUMA. Kaspersky Endpoint Security se pokusí o připojení k serveru na první IP adrese. Pokud připojení nelze navázat, aplikace Kaspersky Endpoint Security se pokusí připojit k druhé IP adrese v seznamu a tak dále.

Úplné šifrování disku

Můžete vybrat technologii šifrování: Kaspersky Disk Encryption nebo BitLocker Drive Encryption (dále označována zkráceně jako „technologie BitLocker“).

Kaspersky Disk Encryption

Technologie Kaspersky Disk Encryption není podporována na počítačích s architekturou ARM.

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 Single Sign-On (SSO), 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 infrastruktury Kaspersky Next. BitLocker šifruje logické svazky. BitLocker nelze použít pro šifrování vyměnitelných jednotek. Podrobnosti o technologii BitLocker najdete v dokumentaci společnosti Microsoft .

Při šifrování disku BitLocker vloží zavaděč a další pomocné soubory do tohoto umístění: system partition. Tento oddíl není šifrován. Operační systém vytvoří systémový oddíl automaticky během instalace systému Windows. Pokud je disk před instalací systému Windows plně rozdělen na oddíly, operační systém nemůže vytvořit systémový oddíl. V tomto případě vás při spuštění šifrování disku BitLocker vyzve operační systém, aby znovu vytvořil oblasti na disku a vytvořil systémový oddíl. Po vytvoření systémového oddílu operační systém spustí šifrování BitLocker.

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 systémového pevného disku musí uživatel před spuštěním operačního systému projít ověřením nástrojem BitLocker. Po ověření umožňuje BitLocker uživateli přihlášení. BitLocker nepodporuje technologii jednotného přihlašování (SSO).

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.

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 možnost, 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 možnost, 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 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.
Nastavení vytváření účtů ověřovacího agenta	**Všechny účty v počítači**. Všechny účty v počítači, které byly kdykoli aktivní. **Všechny účty domén v počítači**. Všechny účty v počítači, které patří do nějaké domény a které byly kdykoli aktivní. **Všechny místní účty v počítači**. Všechny místní účty v počítači, které byly kdykoli aktivní. **Účet služby s jednorázovým heslem**. Účet služby je nezbytný pro získání přístupu k počítači, například když uživatel zapomene heslo. Účet služby můžete také použít jako rezervní účet. Musíte zadat název účtu (ve výchozím nastavení `ServiceAccount`). Kaspersky Endpoint Security vytvoří heslo automaticky. Heslo najdete v konzole aplikace Kaspersky Security Center. **Místní správce**. Kaspersky Endpoint Security vytvoří uživatelský účet ověřovacího agenta pro místního správce počítače. **Správce počítače**. Kaspersky Endpoint Security vytvoří uživatelský účet ověřovacího agenta pro správce počítače. Který účet má roli správce počítače, můžete zjistit ve vlastnostech počítače ve službě Active Directory. Ve výchozím nastavení není role správce počítače definována, to znamená, že neodpovídá žádnému účtu. **Aktivní účet**. Kaspersky Endpoint Security automaticky vytvoří účet ověřovacího agenta pro účet, který je aktivní v době šifrování disku.
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 (zkracuje dobu šifrování)	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 toto nastavení nemění, dokud nejsou dešifrovány pevné disky. 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.

Ve výchozím nastavení není toto políčko zaškrtnuté.

Použít funkci Legacy USB Support (nedoporučuje se)

Pomocí tohoto zaškrtávacího políčka lze povolit nebo zakázat 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. 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.

Použít technologii 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.

Používat u externích poskytovatelů přihlašovacích údajů wrap

Kaspersky Endpoint Security podporuje externího poskytovatele přihlašovacích údajů ADSelfService Plus.

Při práci s externími poskytovateli přihlašovacích údajů zachytí ověřovací agent heslo ještě před načtením operačního systému. To znamená, že uživatel musí zadat heslo pouze jednou při přihlašování do systému Windows. Po přihlášení do systému Windows může uživatel využít možnosti externího poskytovatele přihlašovacích údajů například pro ověřování v podnikových službách. Externí poskytovatelé přihlašovacích údajů také umožňují uživatelům nezávisle resetovat vlastní heslo. V tomto případě aplikace Kaspersky Endpoint Security aktualizuje heslo pro ověřovacího agenta automaticky.

Pokud používáte externího poskytovatele přihlašovacích údajů, který není podporován aplikací, můžete se setkat s určitými omezeními při provozu technologie jednotného přihlašování.

Nápověda

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 možnost, 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 možnost, 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	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 toto nastavení nemění, dokud nejsou dešifrovány pevné disky. 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.

Ve výchozím nastavení není toto políčko zaškrtnuté.

Způsob ověření

Pouze 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.

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.
- **TPM (Trusted Platform Module) nebo heslo, pokud TPM není k dispozici**. Pokud je tato volba vybraná, 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.

Vybranou metodu ověřování je třeba nakonfigurovat zadáním požadavků na heslo nebo PIN:

- **Minimální délka kódu PIN (znaky)**.
- **Minimální délka hesla (znaky)**.
- **Omezit dobu platnosti hesla / kódu PIN pro TPM (dny)**.
- **Povolit používání rozšířeného kódu PIN (písmena a čísla)**. *Rozšířený PIN* umožňuje kromě numerických znaků používat i další znaky: velká a malá písmena latinky, speciální znaky a mezery.

Automaticky znovu vytvořit obnovovací klíč (dny)	Automatická aktualizace hesla pro obnovení přístupu k pevnému disku chráněnému nástrojem BitLocker. Pokud je políčko zaškrtnuto, zadejte dobu platnosti hesla klíče pro obnovení. To pomáhá zabránit opakovanému použití hesla klíče pro obnovení.

Šifrování na úrovni souborů

Šifrování souborů není podporováno na počítačích s architekturou ARM.

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.

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 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
Režim 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. **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.
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**. Soubory ve standardní systémové složce *Oblíbené* 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). • **Vlastní složka**. 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.

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.

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.
Šifrované balíčky	Při vytváření šifrovaných balíčků je třeba splnit požadavky na sílu hesla.

Šifrování vyměnitelných jednotek

Šifrování vyměnitelných jednotek není podporováno na počítačích s architekturou ARM.

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:

- Full Disk Encryption (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).

- File Level Encryption (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
Režim 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.
Přenosný 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.

Vlastní pravidla

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 (Hardware ID neboli HWID)
  - Podle modelu zařízení: Vendor ID (VID) a Product ID (PID)

Povolit šifrování vyměnitelných jednotek 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.

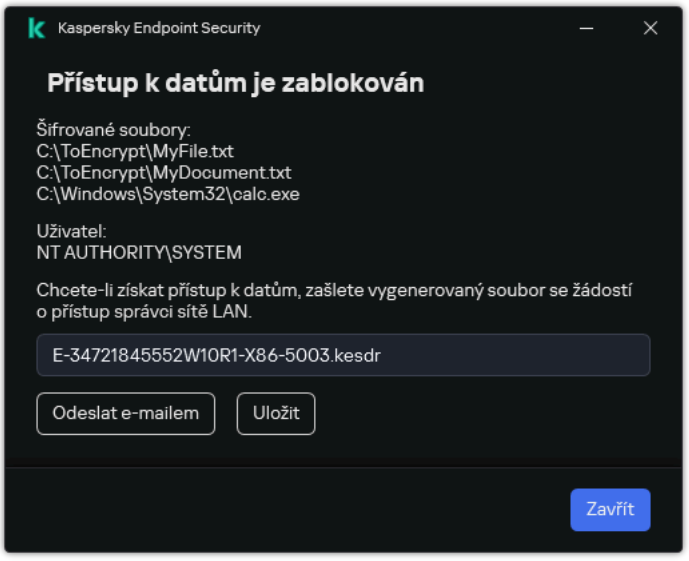
Není-li políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nezašifruje vyměnitelné jednotky bez připojení ke službě Kaspersky Security Center.

Nastavení hesla šifrování / Mobilní správce souborů

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 uživatele**. 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 zónu 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.

U aplikace Kaspersky Endpoint Security pro systém Windows můžete od verze 12.5 přidávat telemetrii EDR do důvěryhodné zóny. To umožňuje optimalizovat data, která aplikace odesílá na server pro shromažďování telemetrie u řešení Kaspersky Anti Targeted Attack Platform (EDR).

Počínaje aplikací Kaspersky Endpoint Security 12.6 pro Windows jsou do důvěryhodné zóny přidány výjimky z kontroly a důvěryhodné aplikace. Předdefinované výjimky z kontroly a důvěryhodné aplikace pomáhají rychle konfigurovat aplikaci Kaspersky Endpoint Security na serverech SQL, serverech Microsoft Exchange a řešení System Center Configuration Manager. To znamená, že nemusíte ručně nastavovat důvěryhodnou zónu pro aplikaci na serverech.

Počínaje aplikací Kaspersky Endpoint Security pro systém Windows verze 12.8 můžete aplikaci nainstalovat v režimu Light Agent za účelem ochrany virtuálních prostředí. Předdefinované výjimky z kontroly a důvěryhodné aplikace vám mohou pomoci rychle nakonfigurovat aplikaci Kaspersky Endpoint Security ve virtuálních prostředích Citrix a VMware.

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 mohou útočníci využívat k poškození počítače nebo osobních dat, najdete na webu 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.
- Úloha *Kontrola malwaru*.

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 monitoruje objekty, které jsou otevírané, spouštěné nebo ukládané jakýmkoli procesem aplikace, a kontroluje činnost všech aplikací a veškerý síťový provoz, který tyto aplikace vygenerují. Po přidání aplikace do seznamu důvěryhodných aplikací přestane aplikace Kaspersky Endpoint Security monitorovat činnost této aplikace.

Rozdíl mezi výjimkami z kontroly a důvěryhodnými aplikacemi je v tom, že u výjimky aplikace Kaspersky Endpoint Security nekontroluje soubory, zatímco u důvěryhodných aplikací nekontroluje spouštěné procesy. Pokud důvěryhodná aplikace vytvoří škodlivý soubor ve složce, která není zahrnuta ve výjimkách z kontroly, aplikace Kaspersky Endpoint Security tento soubor detekuje a hrozbu odstraní. Jestliže je složka přidána do výjimek, Kaspersky Endpoint Security tento soubor přeskočí.

Pokud například považujete objekty používané standardní aplikací Poznámkový blok v systému Microsoft Windows za bezpečnou (tj. této aplikaci důvěřujete), může ji přidat na seznam důvěryhodných aplikací, aby objekty používané touto aplikací nebyly sledovány. To zvýší výkon počítače, což je zvláště důležité při používání serverových aplikací.

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.

Důvěryhodné aplikace pomáhají předcházet problémům s kompatibilitou mezi aplikací Kaspersky Endpoint Security a jinými aplikacemi (například problém dvojité kontroly síťového provozu počítače třetí strany aplikací Kaspersky Endpoint Security a jinou antivirovou 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 zjišťovaných 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 nebezpečí**: 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. *Overwriting* viry přepíší svůj kód přes kód infikovaného souboru, čímž se obsah souboru vymaže. Infikovaný soubor přestane fungovat a nebude možné jej obnovit. *Parasitic* viry upravují soubory a zanechají se plně nebo částečně funkční. *Companion* 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: *Link viry*, *viry OBJ*, *viry LIB*, viry *zdrojového kódu* a mnoho dalších. **Worm** 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. **IM-Worm** / Červi klienta 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. **IRC-Worm** / Červi internetových konverzací / Šíří se prostřednictvím 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. **Net-Worm** / 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.
P2P-Worm	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.
Worm	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 (včetně ransomwaru)

Podkategorie: Trojské koně

Úroveň nebezpečí: 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.
Backdoor	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.
Trojan	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 „útočníkovi“ 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
Constructor	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 nebezpečí: 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: legitimní software, který mohou útočníci použít 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.

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.

- Legitimní software, který mohou použít útočníci k poškození počítače nebo osobních dat

Podkategorie: legitimní software, který mohou útočníci použít 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.
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

  Podkategorie: Zabalené soubory, které mohou způsobit škodu.

  Úroveň nebezpečí: střední.

  Soubor je zabalen pomocí speciálního komprimačního programu, který se používá pro balení malwaru: virů, červů, trojských koní. Aplikace Kaspersky Endpoint Security kontroluje rozbalovací modul v (samorozbalovacích) archivech SFX.

  Aby hackeři skryli malware před detekcí antivirem, zabalí jej pomocí speciálních komprimačních programů. Odborníci společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

- Mnohonásobné komprimované objekty

Podkategorie: Zabalené soubory, které mohou způsobit škodu.

Úroveň nebezpečí: střední.

Soubor je zabalen pomocí speciálního komprimačního programu, který se používá pro balení malwaru: virů, červů, trojských koní. Aplikace Kaspersky Endpoint Security kontroluje rozbalovací modul v (samorozbalovacích) archivech SFX.

Aby hackeři skryli malware před detekcí antivirem, zabalí jej pomocí speciálních komprimačních programů. Odborníci společnosti Kaspersky identifikovali komprimační programy, které jsou mezi hackery nejoblíbenější.

Výjimky

Tato tabulka obsahuje informace o výjimkách z kontroly.

Místo absolutních cest doporučujeme zadávat relativní cesty. To umožňuje vyloučit nejen objekty systému souborů, ale také objekty bez souborů. Například `*\Program Files (x86)\Folder\Subfolder`.

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:\Folder\**\*.txt` bude reprezentovat všechny cesty k souborům s příponou TXT umístěným ve složkách vnořených ve složce `Folder` kromě této složky `Folder` 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:\Folder\???.txt` bude obsahovat cesty ke všem souborům umístěným ve složce s názvem `Folder`, které mají příponu TXT a název skládající se ze tří znaků.

    Masky můžete použít kdekoli v cestě k souboru nebo složce. Chcete-li například, aby rozsah kontroly zahrnoval složku Stažené soubory pro všechny uživatelské účty v počítači, zadejte masku `C:\Users\*\Downloads\`.

    Kaspersky Endpoint Security podporuje proměnné prostředí

    Kaspersky Endpoint Security nepodporuje při generování seznamu výjimek z kontroly 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`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

- 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 vyloučí z kontroly objekty `Client-IRC`, `Client-P2P` a `Client-SMTP`.

Kaspersky Endpoint Security skryje seznam výjimek z kontroly v uživatelském rozhraní aplikace, pokud je konfigurace výjimek z kontroly blokována správcem v konzole (symbol „zavřeného zámku“) a místní výjimky z kontroly jsou zakázány (není zaškrtnuto políčko **Povolit používání místních výjimek**).

Důvěryhodné aplikace

Tato tabulka uvádí důvěryhodné aplikace, jejichž aktivita není aplikací Kaspersky Endpoint Security během činnosti monitorována.

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`). Při každém přidání nové proměnné prostředí musíte aplikaci restartovat.

Součást Kontrola aplikací řídí spouštění všech aplikací, a to bez ohledu na skutečnost, zda je aplikace uvedena v tabulce důvěryhodných aplikací či nikoli.

Kaspersky Endpoint Security skryje konsolidovaný seznam důvěryhodných aplikací v uživatelském rozhraní aplikace, pokud je konfigurace důvěryhodných aplikací blokována správcem v konzole (symbol „zavřeného zámku") a místní důvěryhodné aplikace jsou zakázány (není zaškrtnuto políčko **Povolit používání místních důvěryhodných aplikací**).

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.

Tato funkce také umožňuje slučování seznamů v profilech zásad. Chcete-li sloučit seznamy, povolte v profilu s nejvyšší prioritou dědění nastavení z profilu s nižší prioritou. Další informace o prioritách profilů zásad najdete v nápovědě k aplikaci Kaspersky Security Center.

Povolit používání místních výjimek / Povolit používání místních důvěryhodných aplikací

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

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.

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.

Telemetrie EDR (KATA) / NDR (KATA)

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

Tato tabulka obsahuje informace o výjimkách telemetrie EDR.

Telemetrie KUMA

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

Seznam událostí, které mají být odeslány na platformu Kaspersky Unified Monitoring and Analysis Platform (KUMA). Aplikace Kaspersky Endpoint Security funguje v těchto režimech:

- **Odesílat všechny události**. V tomto režimu aplikace odesílá všechny události z protokolu systému Windows kromě událostí přidaných do pravidel výjimek.
- **Odesílat pouze vybrané události**. V tomto režimu aplikace odesílá pouze události přidané do pravidel zahrnutí.

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 při spuštění počítače (doporučeno)	Pokud je tato možnost vybraná, aplikace Kaspersky Endpoint Security se spustí po načtení operačního systému, čímž počítač chrání během celé relace. Pokud tato není zaškrtnutá, 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 (vyžaduje značné výpočetní prostředky)	Aplikace Kaspersky Endpoint Security obvykle ukončí zjištěný malware předtím, než se počítač infikuje. Pokročilá technologie dezinfekce chrání počítač před již aktivním malwarem (aktivní infekcí), čímž minimalizuje riziko ztráty dat a šíření hrozby. Je-li tato technologie povolena, při zjištění škodlivé aktivity zobrazí Kaspersky Endpoint Security místní upozornění. V oznámení aplikace Kaspersky Endpoint Security nabízí uživateli možnost provedení pokročilé dezinfekce počítače. Jakmile uživatel tento postup schválí, aplikace Kaspersky Endpoint Security hrozbu zneutralizuje a poté restartuje počítač. Technologie pokročilé dezinfekce využívá značné množství výpočetních prostředků, což může jiné aplikace zpomalovat. Když aplikace zjišťuje aktivní infekci, mohou být některé funkce operačního systému nedostupné. Dostupnost operačního systému se obnoví po dokončení pokročilé dezinfekce a restartování počítače. Je-li aplikace Kaspersky Endpoint Security nainstalována v počítači se systémem Windows pro servery, toto upozornění nezobrazí. Nemůžete tak vybrat akci, která dezinfikuje aktivní hrozbu. Chcete-li dezinfikovat hrozbu, musíte v nastavení aplikace povolit technologii pokročilé dezinfekce a v nastavení úlohy *Kontrola malwaru* povolit okamžitou pokročilou dezinfekci. Poté musíte spustit úlohu *Kontrola malwaru*.
Použít Kaspersky Security Center jako proxy server pro aktivaci *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	Pokud je toto zaškrtávací políčko zaškrtnuto, aplikace používá server pro správu Kaspersky Security Center jako proxy server pro připojování k aktivačním serverům. To je nutné, když používáte aktivační kód k aktivaci aplikace v izolovaném segmentu sítě bez přístupu k internetu. Pokud aplikaci aktivujete pomocí souboru klíče, není nutný přístup k internetu.
Povolit sebeobranu	Pokud je tato funkce povolena, aplikace Kaspersky Endpoint Security brání úpravám nebo odstranění souborů aplikace na pevném disku, paměťových procesů a záznamů v systémovém registru.
Blokovat externí správu služeb aplikace	Pokud je tato funkce povolena, Kaspersky Endpoint Security nepovoluje správu služeb aplikace pomocí aplikací třetích stran (například CMD). Pokud dojde k pokusu o vzdálenou správu služeb aplikace pomocí aplikací třetích stran, na hlavním panelu systému Microsoft Windows nad ikonou aplikace se zobrazí oznámení (pokud nebyla oznamovací služba vypnuta uživatelem). Externí správu služeb aplikace můžete povolit pouze v počítačích, které nepodporují technologii AM-PPL, nebo v počítačích, které mají tuto technologii zakázánu.
Odložit naplánované úlohy při napájení z baterie	Je-li toto políčko zaškrtnuto, je povolen režim úspory energie, když je počítač napájen z baterie. Aplikace Kaspersky Endpoint Security plánované úlohy odloží. Úlohy kontroly a aktualizace můžete spustit ručně, je-li třeba. Když je režim úspory energie povolen a počítač je napájen z baterie, následující úlohy nebudou spuštěny ani v případě, že byly naplánované: • *Aktualizace databází a modulů aplikace* • *Úplná kontrola* • *Kontrola kritických oblastí* • *Vlastní kontrola* • *Kontrola integrity aplikací* • *Kontrola IOC*.

Při zatížení přenechat zdroje ostatním aplikacím

Spotřeba prostředků počítače aplikací Kaspersky Endpoint Security při kontrole počítače může zvýšit zatížení subsystémů procesoru a pevného disku. To může zpomalovat jiné aplikace. Pro optimalizaci výkonu poskytuje aplikace Kaspersky Endpoint Security *režim pro přenos prostředků do jiných aplikací*. V tomto režimu může operační systém v případě vysokého zatížení procesoru snížit prioritu vláken úloh kontroly aplikace Kaspersky Endpoint Security. To umožňuje přerozdělit prostředky operačního systému jiným aplikacím. Úlohy kontroly tak získají méně času procesoru. Aplikace Kaspersky Endpoint Security proto bude kontrolovat počítač déle. Aplikace ve výchozím nastavení uvolňuje prostředky pro jiné aplikace.

Omezit využívání procesoru pro úlohy kontroly

Chcete-li optimalizovat výkon aplikace Kaspersky Endpoint Security, můžete omezit využití procesoru pomocí úlohy *Kontrola malwaru*.

Pokud je toto políčko zaškrtnuté, průměrné zatížení všech jader CPU z úlohy *Kontrola malwaru* se přiblíží stanovené hodnotě.

Ve výchozím nastavení není toto políčko zaškrtnuté.

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 následující stavy: *OK*, *Varování* a *Kritický*.

Instalovat aktualizace bez restartování počítače

Upgrade aplikace bez restartování počítače umožňuje zajistit nepřetržitý provoz serverů.

Aplikaci můžete upgradovat bez restartu od verze 11.10.0. Chcete-li upgradovat starší verzi aplikace, musíte restartovat počítač.

Počínaje verzí 11.11.0 můžete provádět následující akce bez restartování počítače:

- instalovat bezpečnostní opravy,
- měnit sadu součástí aplikace,
- instalovat aplikaci Kaspersky Endpoint Security přes Kaspersky Security for Windows Server.

Výchozí hodnota parametru se liší v závislosti na typu operačního systému. Pokud je aplikace nainstalována na pracovní stanici, možnost upgradu aplikace bez restartu je zakázána. Jestliže je aplikace nainstalována na serveru, možnost upgradu aplikace bez restartu je povolena.

Kompatibilita se softwarem pro vzdálenou správu

(k dispozici pouze v konzole aplikace Kaspersky Security Center)

Pokud používání aplikace Kaspersky Endpoint Security spolu s nástroji pro vzdálenou správu (RAT) způsobuje problémy, můžete povolit režim kompatibility. Problémy mohou souviset s nekompatibilitou RAT s funkcí Secure Desktop aplikace. Účelem této funkce je potvrzovat akce, které mohou potenciálně snížit úroveň zabezpečení počítače. Tato funkce umožňuje aplikaci zobrazit potvrzovací dialog, který je izolován od ostatních procesů. Tato funkce používá k zabezpečení požadavku oprávnění vyšší úrovně. Akci tak může potvrdit pouze uživatel, nikoli malware.

Pokud je tato možnost vybrána, je režim kompatibility RAT povolen. Aplikace zobrazí potvrzovací dialog bez této funkce. Může to snížit úroveň zabezpečení počítače. Nedoporučujeme zapínat režim kompatibility, pokud Kaspersky Endpoint Security nezpůsobuje problémy s vaším RAT.

Pokud tato možnost není vybrána, režim kompatibility RAT je zakázán. Ve výchozím nastavení není toto políčko zaškrtnuté.

Příklad: Při používání prohlížeče v režimu RemoteApp nemusí aplikace Kaspersky Endpoint Security zobrazit potvrzovací okno při návštěvě webu s nedůvěryhodným certifikátem, protože aplikace RemoteApp nepodporuje funkci Secure Desktop aplikace. To může způsobit, že prohlížeč přestane reagovat. Aby prohlížeč správně fungoval v režimu RemoteApp, musíte povolit režim kompatibility. Můžete také zkusit povolit režim kompatibility, pokud narazíte na problémy s funkcí Secure Desktop při používání jiného softwaru třetí strany.

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.14.0\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.14.0\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.

Karanténa

Karanténa je speciální místní úložiště v počítači. Uživatel může umístit do karantény soubory, které považuje za nebezpečné pro počítač. Soubory v karanténě jsou uloženy v šifrovaném stavu a neohrožují zabezpečení zařízení. Aplikace Kaspersky Endpoint Security použije karanténu, pouze je-li integrována s řešeními Kaspersky Detection and Response. V ostatních případech aplikace Kaspersky Endpoint Security umístí příslušný soubor do zálohy. Podrobnosti o správě karantény jako součásti řešení najdete v nápovědě k řešení Kaspersky Sandbox, nápovědě k řešení Kaspersky Endpoint Detection and Response Optimum, nápovědě k řešení Kaspersky Endpoint Detection and Response Expert, nápovědě k řešení Kaspersky Anti Targeted Attack Platform a nápovědě k řešení Kaspersky Endpoint Detection and Response Expert (on-premise).

Karanténu lze konfigurovat pouze pomocí webové konzoly. Webovou konzolu můžete také použít ke správě objektů v karanténě (obnovení, odstranění, přidání atd.). Objekty můžete obnovit místně v počítači pomocí příkazového řádku.

Kaspersky Endpoint Security používá ke karanténě souborů systémový účet (SYSTEM).

Nastavení zpráv a úložiště

Parametr	Popis
Delete reports after (days)	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 aplikace Kaspersky Endpoint Security automaticky mazat nejstarší záznamy ze souboru zprávy.
Limit the size of report file to (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.
Delete objects after (days)	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.
Limit the size of Backup to (MB)	Pokud je toto políčko zaškrtnuto, maximální velikost úložiště je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost nastavena na 1024 MB. Aby nedošlo k překročení maximální velikosti úložiště, bude aplikace Kaspersky Endpoint Security po dosažení maximální velikosti úložiště automaticky z úložiště odstraňovat nejstarší soubory.
Limit the size of Quarantine	Pokud je toto políčko zaškrtnuto, maximální velikost karantény je omezena na definovanou hodnotu. Ve výchozím nastavení je maximální velikost nastavena na 1024 MB. Když karanténa dosáhne maximální velikosti, aplikace Kaspersky Endpoint Security odešle do aplikace Kaspersky Security Center událost *Nedostatek místa v úložišti karantény* a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace zastaví ukládání nových objektů do karantény. Karanténu musíte vyprazdňovat ručně.
Notify when the Quarantine storage reaches (%)	Prahová hodnota karantény. Můžete například nastavit prahovou hodnotu karantény na 50 %. Když karanténa dosáhne prahové hodnoty, aplikace Kaspersky Endpoint Security odešle odpovídající událost do aplikace Kaspersky Security Center a zveřejní událost v protokolu událostí systému Windows. Mezitím aplikace pokračuje v ukládání nových objektů do karantény.
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. Za účelem optimalizace místa na disku na serveru pro správu můžete zakázat přenos některých dat. Aplikace odesílá události následujících kategorií: • **About Quarantine files**. Seznam souborů v karanténě můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Repositories** → **Quarantine**. Aplikace Kaspersky Endpoint Security použije karanténu, pouze je-li integrována s řešeními Kaspersky Detection and Response. • **About files in Backup**. Seznam souborů v záloze můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Repositories** → **Backup**. • **About unprocessed files**. Seznam nezpracovaných souborů můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Repositories** → **Active threats**. • **About installed devices**. Seznam připojených zařízení můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Repositories** → **Hardware**. Seznam zařízení je k dispozici také ve vlastnostech počítače a v zásadách aplikace Kaspersky Endpoint Security pro systém Windows (část **Kontrola zařízení**). • **About started applications**. Seznam spustitelných souborů můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Application management** → **Executable files**. Seznam spustitelných souborů je k dispozici také ve vlastnostech počítače.

- **About file encryption errors**. Seznam chyb šifrování souborů můžete zobrazit v konzole aplikace Kaspersky Security Center ve složce **Advanced** → **Data encryption and protection** → **Encryption events**. Seznam chyb je k dispozici také ve vlastnostech počítače.
- **Report on Adaptive Anomaly Control rules state**. Zprávu můžete zobrazit v konzole aplikace Kaspersky Security Center v uzlu **Administration Server** na kartě **Reports**. Tato zpráva je k dispozici také ve vlastnostech zásad aplikace Kaspersky Endpoint Security pro systém Windows (část **Adaptivní kontrola anomálií**).
- **Report on triggered Adaptive Anomaly Control rules**. Zprávu můžete zobrazit v konzole aplikace Kaspersky Security Center v uzlu **Administration Server** na kartě **Reports**. Tato zpráva je k dispozici také ve vlastnostech zásad aplikace Kaspersky Endpoint Security pro systém Windows (část **Adaptivní kontrola anomálií**).
- **About a threat development chain**. Podrobnosti o zjištěních můžete zobrazit ve webové konzole aplikace Kaspersky Security Center v části **Monitoring** → **Alerts**. Informace o řetězci vývoje hrozeb využívá řešení Kaspersky Endpoint Detection and Response.

Nastavení sítě

Můžete nakonfigurovat proxy server používaný pro připojení k internetu a aktualizaci antivirových databází, vybrat režim monitorování síťových portů a nastavit 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.
Vkládat 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.
Nastavení proxy serveru	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 použije adresu proxy serveru zadanou v nastavení prohlížeče Microsoft Internet Explorer.
Obcházet proxy server u místních adres	Je-li toto políčko zaškrtnuto, aplikace Kaspersky Endpoint Security nepoužije proxy serveru při provádění aktualizace ze sdílené složky.
Nastavení autentifikace proxy serveru	Chcete-li ověřit aplikaci na proxy serveru pro přístup k internetu, je nutné zadat přihlašovací údaje uživatele. Kaspersky Endpoint Security podporuje automatické ověření na proxy serveru. Pokud automatické ověření selhalo, aplikace vás vyzve k zadání přihlašovacích údajů. **Nepoužívat ověřování**. **Ověřování NTLM**. Ověřování NTLM aktuálním uživatelským účtem (výchozí). **Ověřování NTLM pomocí uživatelského jména a hesla**. Ověřování NTLM pomocí ručně zadaných přihlašovacích údajů. **Uživatelské jméno a heslo**. Ověřování pomocí ručně zadaných přihlašovacích údajů. **Automatické ověření**. **Ověřování protokolem Kerberos**. Ověřování protokolem Kerberos aktuálním uživatelským účtem. Aby ověření protokolem Kerberos fungovalo správně při používání záznamů CNAME pro adresu proxy serveru, musíte pro každý záznam CNAME zaregistrovat hlavní název služby (SPN). **Ověřování protokolem Kerberos pomocí uživatelského jména a hesla**. Ověřování protokolem Kerberos pomocí ručně zadaných přihlašovacích údajů. Pokud je vybráno ověřování protokolem Kerberos, může Kaspersky Endpoint Security v závislosti na nastavení proxy serveru provádět ověřování pomocí protokolu Kerberos nebo NTLM.
Sledované porty	**Sledovat všechny síťové porty**. V tomto režimu sledování síťových portů součásti ochrany (Ochrana před souborovými hrozbami, Ochrana před webovými hrozbami a 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 webovými 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.

Důvěryhodné kořenové certifikáty

Seznam důvěryhodných kořenových certifikátů. Aplikace Kaspersky Endpoint Security umožňuje instalovat do uživatelských počítačů důvěryhodné kořenové certifikáty, pokud například potřebujete nasadit nové certifikační centrum. Aplikace umožňuje přidat certifikát do speciálního úložiště certifikátů Kaspersky Endpoint Security. V tomto případě je certifikát považován za důvěryhodný pouze pro aplikaci Kaspersky Endpoint Security. Jinými slovy, uživatel může získat přístup k webu s novým certifikátem v prohlížeči. Pokud se k webovému serveru pokusí získat přístup jiná aplikace, může dojít k chybě připojení z důvodu problému s certifikátem. K přidání do systémového úložiště certifikátů můžete použít zásady skupin služby Active Directory.

Návštěva domény s nedůvěryhodným certifikátem

- **Povolit**. 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.

  Pokud aplikace nebo služba třetí strany naváže spojení s doménou s nedůvěryhodným certifikátem, Kaspersky Endpoint Security vytvoří svůj vlastní certifikát pro kontrolu provozu. Nový certifikát má stav *Nedůvěryhodné*. To je nutné pro upozornění aplikace třetí strany na nedůvěryhodné připojení, protože v tomto případě nelze zobrazit stránku HTML a připojení lze navázat v režimu na pozadí.

- **Blokovat**. Při návštěvě domény s nedůvěryhodným certifikátem aplikace Kaspersky Endpoint Security zablokuje 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.

Návštěva domény s chybou kontroly šifrovaných připojení

- **Blokovat**. Pokud je vybrána tato položka, aplikace Kaspersky Endpoint Security při výskytu chyby kontroly šifrovaného připojení blokuje síťové připojení.
- **Povolit a přidat doménu k výjimkám**. 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**. Kaspersky Endpoint Security také vytvoří událost pro chybu kontroly šifrovaného připojení.

Blokovat připojení SSL 2.0

Pokud je políčko zaškrtnuto, aplikace monitoruje a blokuje síťová připojení vytvořená pomocí protokolu SSL 2.0.

Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu SSL 2.0. Aplikace však nemonitoruje síťový provoz přes tento protokol.

Blokovat připojení SSL 3.0

Pokud je políčko zaškrtnuto, aplikace blokuje síťová připojení vytvořená pomocí protokolu SSL 3.0.

Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu SSL 3.0. Aplikace monitoruje síťový provoz přes tento protokol. Všechny součásti aplikace fungují bez omezení.

Blokovat připojení TLS 1.0	Pokud je políčko zaškrtnuto, aplikace blokuje síťová připojení vytvořená pomocí protokolu TLS 1.0. Pokud políčko není zaškrtnuto, aplikace neblokuje síťová připojení vytvořená pomocí protokolu TLS 1.0. Aplikace monitoruje síťový provoz přes tento protokol. Všechny součásti aplikace fungují bez omezení.
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 dešifruje a monitoruje šifrovaná připojení a weby, které používají certifikát EV. Jestliže toto políčko není zaškrtnuté, aplikace nemá přístup k obsahu provozu HTTPS. Z tohoto důvodu aplikace monitoruje provoz HTTPS pouze na základě adresy webových stránek, například `https://bing.com`. Pokud poprvé otevíráte web s certifikátem EV, šifrované připojení bude dešifrováno bez ohledu na to, zda je toto políčko zaškrtnuto.
Konfigurovat důvěryhodné adresy	Tato funkce používá seznam webových adres, u kterých aplikace Kaspersky Endpoint Security nekontroluje síťová připojení. V tomto případě Kaspersky Endpoint Security nekontroluje HTTPS provoz důvěryhodných webových adres, když součásti Ochrana před webovými hrozbami, Ochrana před hrozbami v poště a Kontrola webu vykonávají svoji práci. Můžete zadat název domény nebo IP adresu. Kaspersky Endpoint Security podporuje `*` znak pro zadání masky v názvu domény. Aplikace Kaspersky Endpoint Security nepodporuje symbol `*` pro IP adresy. Můžete vybrat rozsah IP adres pomocí masky podsítě (například 198.51.100.0/24). Příklady: • `domain.com` – záznam obsahuje následující adresy: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Záznam neobsahuje subdomény (např. `subdomain.domain.com`). • `subdomain.domain.com` – záznam obsahuje následující adresy: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`. • `*.domain.com` – záznam obsahuje následující adresy: `https://movies.domain.com`, `https://images.domain.com/page123`. Záznam nezahrnuje doménu `domain.com`.
Konfigurovat 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 `?`.
Pokud chcete kontrolovat šifrovaná připojení v aplikacích pomocí jejich vlastního úložiště certifikátů, použijte *(k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security)*	Pokud je toto políčko zaškrtnuto, aplikace 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 nekontroluje šifrovaný provoz v prohlížeči Mozilla Firefox a poštovním klientovi Thunderbird. Aplikace používá k dešifrování a analýze šifrovaného provozu kořenový certifikát Kaspersky. Můžete vybrat úložiště certifikátů, které bude obsahovat kořenový certifikát Kaspersky. • **Úložiště certifikátů Windows (doporučeno)**. Kořenový certifikát společnosti Kaspersky bude přidán do tohoto úložiště během instalace aplikace Kaspersky Endpoint Security. • **Vlastní úložiště certifikátů**. 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)*	**Zobrazit zjednodušené rozhraní**. 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. **Zobrazit uživatelské rozhraní**. 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.

	Skrýt část Monitor aktivity aplikací. Na klientském počítači není v hlavním okně aplikace Kaspersky Endpoint Security tlačítko **Monitor aktivity aplikací** k dispozici. *Monitor aktivity aplikací* je nástroj navržený k zobrazování informací o aktivitě aplikací uživatelského počítače v reálném čase. **Nezobrazovat uživatelské rozhraní**. V klientském počítači se nezobrazují žádné známky provozu aplikace Kaspersky Endpoint Security. Ikona v oznamovací oblasti systému Windows ani upozornění nejsou k dispozici.
Konfigurovat 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.
Konfigurovat upozornění e-mailem	Nastavení SMTP serveru pro doručování upozornění na události zjištěné během provozu aplikace. Ve výchozím nastavení používá Kaspersky Endpoint Security nastavení upozornění e-mailem z aplikace Kaspersky Security Center. Další informace o nastavení upozornění e-mailem najdete v nápovědě k aplikaci Kaspersky Security Center. Pokud potřebujete nakonfigurovat jednotlivá e-mailová upozornění, můžete upravit následující nastavení: • **Adresa odesílatele**. E-mailová adresa odesílatele. Použití neexistující adresy se nedoporučuje. • **Server SMTP**. Jedna nebo více adres e-mailových serverů vaší organizace (např. `mail.company.com`). Můžete zadat IP adresu (IPv4 nebo IPv6). Chcete-li ověřit uživatele na serveru SMTP, zadejte do příslušných polí přihlašovací údaje odesílatele. Chcete-li otestovat e-mailová upozornění, můžete odeslat zkušební zprávu. • **Adresa příjemce**. E-mailové adresy příjemců, kterým bude aplikace zasílat upozornění. • **Režim odeslání**. Režim odesílání e-mailových upozornění. Kaspersky Endpoint Security může odesílat zprávy okamžitě, když dojde k události; alternativně může postupovat podle předem nakonfigurovaného plánu.
Zobrazovat stav 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 antimalwarové 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 účet KLAdmin.
Uživatelská podpora / Odkazy na webové prostředky *(k dispozici pouze v konzole aplikace Kaspersky Security Center)*	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.
Uživatelská podpora / Popis *(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 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	Kdykoli můžete obnovit nastavení aplikace doporučené společností Kaspersky. Po obnovení nastavení bude pro všechny součásti ochrany nastavena **Doporučená** úroveň zabezpečení.

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.

Aktualizační funkce (včetně poskytování aktualizací antivirových signatur a aktualizací báze kódů) nemusí být v softwaru dostupná na území USA.

Pravidelné aktualizace vyžadují platnou licenci. Pokud nemáte k dispozici žádnou licenci, aktualizaci budete moci provést jen jednou.

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.

Pokud jsou databáze zastaralé, balíček aktualizace může být velký, což může způsobit dodatečný internetový provoz (až několik desítek MB).

Informace o aktuálním stavu databází Kaspersky Endpoint Security se zobrazují v hlavním okně aplikace nebo v popisku, který se zobrazí, když umístíte kurzor na ikonu aplikace v oznamovací oblasti.

Informace o výsledcích aktualizace a všech událostech, k nimž dojde během aktualizace, jsou zaznamenávány do zprávy aplikace Kaspersky Endpoint Security.

Pokud aplikace funguje v režimu Light Agent, při aktualizaci databází a modulů aplikace je třeba brát zvláštní ohledy.

Nastavení aktualizace modulů a databází aplikace

Parametr	Popis
Plán aktualizace databází	**Automaticky**. V tomto režimu aplikace 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. **Manually**. Tento režim spuštění úlohy aktualizace umožňuje spustit úlohu aktualizace ručně. **By schedule**. 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.
Run missed tasks	Pokud je toto políčko zaškrtnuto, spustí aplikace Kaspersky Endpoint Security vynechanou úlohu, jakmile to bude možné. Úlohu lze vynechat, například pokud byl počítač vypnut v době naplánovaného spuštění úlohy. Když aplikace dostane příležitost provést zmeškané úlohy, spustí úlohy náhodně v určitém časovém intervalu, aby se rozložilo zatížení počítače. Jestliže je zaškrtnutí tohoto políčka zrušeno, aplikace Kaspersky Endpoint Security přeskočené úlohy nespustí. Provede místo toho další aktuálně naplánovanou úlohu.
Zdroje aktualizací	*Aktualizační zdroj* 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.

Pokud nejsou aktualizační servery Kaspersky dostupné, Kaspersky Endpoint Security může k aktualizaci databází a modulů aplikačního softwaru použít alternativní domény. Podrobné informace naleznete ve znalostní bázi technické podpory.

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.

Ve výchozím nastavení používá Kaspersky Endpoint Security jako první zdroj aktualizací server Kaspersky Security Center. To pomáhá šetřit provoz při aktualizaci. Pokud na počítač nejsou aplikovány zásady, jako první zdroj aktualizací jsou v nastavení místní úlohy *Aktualizace databází a modulů aplikace* vybrány servery společnosti Kaspersky, protože aplikace nemusí mít přístup k serveru Kaspersky Security Center.

Pokud je aplikace spuštěna v režimu Light Agent, jako aktualizační zdroj je vybrána složka na SVM.

Spouštět aktualizace databází 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 aplikace můžete určit uživatele, který potřebná oprávnění má, a spustit úlohu aktualizace aplikace Kaspersky Endpoint Security v rámci účtu tohoto uživatele.

Stahovat aktualizace modulů aplikace

Stahování aktualizací modulu aplikace s aktualizacemi databáze aplikace.

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.14.0\Update distribution\`.

Proxy server pro aktualizace

(k dispozici pouze v rozhraní aplikace Kaspersky Endpoint Security)

Nastavení proxy serveru pro přístup uživatelů klientských počítačů k internetu za účelem aktualizace modulů a databází 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.

Obcházet proxy server u místních adres

(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 – informační soubor programu (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

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 – informační soubor programu (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

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 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 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`
`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`
	Aktualizace databází a softwarových modulů aplikace.

`downloads.upd.kaspersky.com` Protokol: `HTTPS` Port: `443`	• Aktualizace databází a softwarových modulů aplikace. • Ověření přístupu k serverům společnosti Kaspersky. 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, když je spuštěna součást Ochrana před webovými hrozbami.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Protokol: `HTTP`
Port: `80`
	Aktualizace databází a softwarových modulů aplikace.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protokol: `HTTPS`
Port: `443`
	Používání služby Kaspersky Security Network

`ksn-a-stat-geo.kaspersky-labs.com` `ksn-file-geo.kaspersky-labs.com`	Používání služby Kaspersky Security Network

`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: `KSN`
Port: `443`, `1443`	

`click.kaspersky.com`	Postupujte podle odkazů z rozhraní.
`redirect.kaspersky.com` Protokol: `HTTPS` Port: `443`	

Nastavení, používá se k šifrování

Adresa	Popis

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokol: `HTTP`
Port: `80`
	Infrastruktura veřejného klíče (PKI).

Příloha 6. Události aplikace

V protokolu událostí aplikace Kaspersky Security Center a protokolu událostí systému Windows jsou zaznamenávány informace o provozu každé součásti aplikace Kaspersky Endpoint Security, událostech šifrování dat, dokončení každé úlohy kontroly malwaru, úlohy aktualizace, úlohy kontroly integrity a také o celkovém fungování aplikace.

Kaspersky Endpoint Security generuje události těchto typů: obecné a konkrétní. Konkrétní události vytváří pouze aplikace Kaspersky Endpoint Security pro systém Windows. Konkrétní události mají jednoduché ID, například `000000cb`. Konkrétní události obsahují následující povinné parametry:

- `GNRL_EA_DESCRIPTION` je obsah události.
- `GNRL_EA_ID` je ID služby události.
- `GNRL_EA_SEVERITY` je stav události. `1` – *Info*, `2` – *Warning*, `3` – *Functional failure*, `4` – *Critical*.
- `EVENT_TYPE_DISPLAY_NAME` je název události.
- `TASK_DISPLAY_NAME` je název součásti aplikace, která příslušnou událost iniciovala.

Obecné události může vytvářet aplikace Kaspersky Endpoint Security pro systém Windows i další aplikace společnosti Kaspersky (například Kaspersky Security for Windows Server). Obecné události mají složitější ID, například `GNRL_EV_VIRUS_FOUND`. Kromě povinného nastavení obsahují obecné události rozšířené nastavení.

Jak dlouho jsou události uloženy na serveru

Kritické

Rozbalit vše | Sbalit vše

License expired

Stav	!
Součást	Audit systému
ID události systému Windows	201
ID události aplikace Kaspersky Security Center	GNRL_EV_LICENSE_EXPIRATION
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

License has almost expired

Stav	!
Součást	Audit systému
ID události systému Windows	203
ID události aplikace Kaspersky Security Center	000000cb
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Databases are missing or corrupted

Stav	!
Součást	Audit systému
ID události systému Windows	206
ID události aplikace Kaspersky Security Center	000000ce
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Databases are extremely out of date

Stav	!
Součást	Audit systému
ID události systému Windows	207
ID události aplikace Kaspersky Security Center	000000cf
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application autorun is disabled

Stav	!
Součást	Audit systému
ID události systému Windows	209
ID události aplikace Kaspersky Security Center	000000d1
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Activation error

Stav	!
Součást	Audit systému
ID události systému Windows	229
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Active threat detected. Advanced Disinfection should be started

Stav	!
Součást	Audit systému
ID události systému Windows	231
ID události aplikace Kaspersky Security Center	000000e7
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

KSN servers unavailable

Stav	!
Součást	Audit systému
ID události systému Windows	2023
ID události aplikace Kaspersky Security Center	000007e7
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Not enough space in Quarantine storage

Stav	!
Součást	Audit systému
ID události systému Windows	343
ID události aplikace Kaspersky Security Center	00000157
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object not restored from Quarantine

Stav	!
Součást	Audit systému
ID události systému Windows	346
ID události aplikace Kaspersky Security Center	0000015a
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object not deleted from Quarantine

Stav	!

Součást	Audit systému
ID události systému Windows	348
ID události aplikace Kaspersky Security Center	0000015c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The application established a connection to a website with an untrusted certificate

Stav	⊗
Součást	Audit systému
ID události systému Windows	57
ID události aplikace Kaspersky Security Center	00000039
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Failed to verify an encrypted connection. The domain is added to the list of exclusions

Stav	⊗
Součást	Audit systému
ID události systému Windows	60
ID události aplikace Kaspersky Security Center	0000003c
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Malicious object detected (local bases)

Stav	⊗
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Prevence narušení hostitele Detekce chování Anti-Cryptor Prevence zneužití Kontrola malwaru
ID události systému Windows	302
ID události aplikace Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Parametry události	• GNRL_EA_PARAM_1 je hash objektu (SHA256). • GNRL_EA_PARAM_2 je název objektu. Když je zjištěno externí šifrování sdílených složek, aplikace ukazuje cestu k cílovému souboru. • GNRL_EA_PARAM_5 je název hrozby dle klasifikace společnosti Kaspersky, např. EICAR-Test-File.

	• `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Malicious object detected (KSN)

Stav	!
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Prevence narušení hostitele Detekce chování Anti-Cryptor Prevence zneužití Kontrola malwaru
ID události systému Windows	`302`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Disinfection impossible

Stav	!

Součást	Ochrana před souborovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Detekce chování Anti-Cryptor Kontrola malwaru
ID události systému Windows	`312`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Cannot be deleted

Stav	!
Součást	Ochrana před souborovými hrozbami Prevence narušení hostitele Detekce chování Anti-Cryptor Kontrola malwaru
ID události systému Windows	`313`
ID události aplikace Kaspersky Security Center	`00000139`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Processing error

Stav	!
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Ochrana AMSI Kontrola malwaru
ID události systému Windows	`317`
ID události aplikace Kaspersky Security Center	`0000013d`

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process terminated

Stav	!
Součást	Ochrana před souborovými hrozbami Prevence narušení hostitele Detekce chování Kontrola malwaru
ID události systému Windows	`452`
ID události aplikace Kaspersky Security Center	`000001c4`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Unable to terminate process

Stav	!
Součást	Ochrana před souborovými hrozbami Prevence narušení hostitele Detekce chování Kontrola malwaru
ID události systému Windows	`453`
ID události aplikace Kaspersky Security Center	`000001c5`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Dangerous link blocked

Stav	!
Součást	Ochrana před webovými hrozbami
ID události systému Windows	`362`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_AND_BLOCKED`
Parametry události	• `GNRL_EA_PARAM_2` je cesta k příslušnému objektu. • `GNRL_EA_PARAM_5` je název objektu podle klasifikace společnosti Kaspersky. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná privátní KSN (`blacklist`): `true` nebo `false`.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Dangerous link opened

Stav	⚠
Součást	Ochrana před webovými hrozbami
ID události systému Windows	`363`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_AND_REPORTED`
Parametry události	• `GNRL_EA_PARAM_2` je cesta k příslušnému objektu. • `GNRL_EA_PARAM_5` je název objektu podle klasifikace společnosti Kaspersky. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná privátní KSN (`blacklist`): `true` nebo `false`.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Previously opened dangerous link detected

Stav	⚠
Součást	Ochrana před webovými hrozbami
ID události systému Windows	`1201`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_AND_PASSED`
Parametry události	• `GNRL_EA_PARAM_2` je cesta k příslušnému objektu. • `GNRL_EA_PARAM_5` je název objektu podle klasifikace společnosti Kaspersky. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná privátní KSN (`blacklist`): `true` nebo `false`.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process action blocked

Stav	⚠
Součást	Adaptivní kontrola anomálií
ID události systému Windows	`2200`

ID události aplikace Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametry události	• `GNRL_EA_PARAM_1` je název pravidla součásti Adaptivní kontrola anomálií. • `GNRL_EA_PARAM_2` je ID heuristického pravidla. • `GNRL_EA_PARAM_3` je jméno uživatele relace. • `GNRL_EA_PARAM_4` je zdrojový proces. • `GNRL_EA_PARAM_5` je zdrojový objekt. • `GNRL_EA_PARAM_6` je cílový proces. • `GNRL_EA_PARAM_7` je cílový objekt. • `GNRL_EA_PARAM_8` jsou další informace o detekovaném objektu: Kontrolní součty zdrojového procesu/objektu a cílového procesu/objektu. Proces zablokován (`verdict_type`): `true` nebo `false`. ID zabezpečení uživatele (SID).
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Keyboard not authorized

Stav	⊗
Součást	Ochrana před útoky BadUSB
ID události systému Windows	`2051`
ID události aplikace Kaspersky Security Center	`00000803`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

AMSI request was blocked

Stav	⊗
Součást	Ochrana AMSI
ID události systému Windows	`2200`
ID události aplikace Kaspersky Security Center	`00000898`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network activity blocked

Stav	⊗
Součást	Brána firewall
ID události systému Windows	`602`
ID události aplikace Kaspersky Security Center	`00000329`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network attack detected

Stav	⚠
Součást	Ochrana před síťovými hrozbami
ID události systému Windows	651
ID události aplikace Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
Parametry události	• GNRL_EA_PARAM_1 je název útoku. • GNRL_EA_PARAM_2 je protokol. • GNRL_EA_PARAM_3 je IP adresa počítače jednajícího jako zdroj síťového útoku. IP adresu udává pořadí bajtů hostitele. Například 2886729929 pro 172.16.0.201. • GNRL_EA_PARAM_4 je číslo portu. • GNRL_EA_PARAM_5 je adresa IPv6, např. 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 je IP adresa počítače, na který cílí síťový útok. IP adresu udává pořadí bajtů hostitele. Například 2886729929 pro 172.16.0.201.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application startup prohibited

Stav	⚠
Součást	Kontrola aplikací
ID události systému Windows	702
ID události aplikace Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
Parametry události	• GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je ručně vytvořený identifikátor kategorie. • GNRL_EA_PARAM_4 je ID kategorie aplikace. • GNRL_EA_PARAM_5 jsou údaje o digitálním podpisu aplikace. • GNRL_EA_PARAM_6 je název spustitelného souboru aplikace (například chrome.exe). • GNRL_EA_PARAM_7 je cesta ke spustitelnému souboru. • GNRL_EA_PARAM_8 je hash objektu (SHA256). • GNRL_EA_PARAM_9 je verze aplikace, kterou se uživatel pokouší spustit.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

Stav	⚠
Součást	Kontrola aplikací
ID události systému Windows	710

ID události aplikace Kaspersky Security Center	000002c6
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Access denied (local bases)

Stav	ⓘ
Součást	Kontrola webu
ID události systému Windows	752
ID události aplikace Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
Parametry události	• GNRL_EA_PARAM_1 je URL. • GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je název pravidla součásti Kontrola webu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Access denied (KSN)

Stav	ⓘ
Součást	Kontrola webu
ID události systému Windows	752
ID události aplikace Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
Parametry události	• GNRL_EA_PARAM_1 je URL. • GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je název pravidla součásti Kontrola webu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Operation with the device prohibited

Stav	ⓘ
Součást	Kontrola zařízení
ID události systému Windows	802
ID události aplikace Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametry události	• GNRL_EA_PARAM_1 je ID hardwaru (HWID). • GNRL_EA_PARAM_2 je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network connection blocked

Stav	
Součást	Kontrola zařízení
ID události systému Windows	809
ID události aplikace Kaspersky Security Center	00000329
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error updating component

Stav	
Součást	Aktualizace
ID události systému Windows	1011
ID události aplikace Kaspersky Security Center	000003f3
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error distributing component updates

Stav	
Součást	Aktualizace
ID události systému Windows	1012
ID události aplikace Kaspersky Security Center	000003f4
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Local update error

Stav	
Součást	Aktualizace
ID události systému Windows	1014
ID události aplikace Kaspersky Security Center	000003f6
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Network update error

Stav	
Součást	Aktualizace
ID události systému Windows	1015
ID události aplikace Kaspersky Security Center	000003f7
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Cannot start two tasks at the same time

Stav	!
Součást	Aktualizace
ID události systému Windows	1017
ID události aplikace Kaspersky Security Center	000003f9
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error verifying application databases and modules

Stav	!
Součást	Aktualizace
ID události systému Windows	1018
ID události aplikace Kaspersky Security Center	000003fa
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error in interaction with Kaspersky Security Center

Stav	!
Součást	Aktualizace
ID události systému Windows	1019
ID události aplikace Kaspersky Security Center	000003fb
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Not all components were updated

Stav	!
Součást	Aktualizace
ID události systému Windows	1021
ID události aplikace Kaspersky Security Center	000003fd
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Update completed successfully, update distribution failed

Stav	!

Součást	Aktualizace
ID události systému Windows	1023
ID události aplikace Kaspersky Security Center	000003ff
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Internal task error

Stav	
Součást	Audit systému
ID události systému Windows	101
ID události aplikace Kaspersky Security Center	00000065
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Patch installation failed

Stav	
Součást	Aktualizace
ID události systému Windows	2153
ID události aplikace Kaspersky Security Center	00000869
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Patch rollback failed

Stav	
Součást	Aktualizace
ID události systému Windows	2156
ID události aplikace Kaspersky Security Center	0000086c
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error applying file encryption / decryption rules

Stav	
Součást	Šifrování dat
ID události systému Windows	904
ID události aplikace Kaspersky Security Center	00000388
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File encryption / decryption error

Stav	!
Součást	Šifrování dat
ID události systému Windows	912
ID události aplikace Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
Parametry události	• GNRL_EA_PARAM_1 je cesta k souboru. • GNRL_EA_PARAM_2 je důvod chyby. • GNRL_EA_PARAM_3 je typ zařízení.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File access blocked

Stav	!
Součást	Šifrování dat
ID události systému Windows	940
ID události aplikace Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
Parametry události	• GNRL_EA_PARAM_1 je cílový objekt. • GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je název spustitelného souboru aplikace (například chrome.exe), který se pokouší získat přístup k souboru.
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Error enabling portable mode

Stav	!
Součást	Šifrování dat
ID události systému Windows	951
ID události aplikace Kaspersky Security Center	000003b7
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error disabling portable mode

Stav	!
Součást	Šifrování dat
ID události systému Windows	953

ID události aplikace Kaspersky Security Center	000003b9
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error creating encrypted package

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	931
ID události aplikace Kaspersky Security Center	000003a3
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error encrypting / decrypting device

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1305
ID události aplikace Kaspersky Security Center	00000519
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Could not load encryption module

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1311
ID události aplikace Kaspersky Security Center	0000051f
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The task for managing Authentication Agent accounts ended with an error

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1340
ID události aplikace Kaspersky Security Center	0000053c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Policy cannot be applied

Stav	!
Součást	Audit systému
ID události systému Windows	1312
ID události aplikace Kaspersky Security Center	00000520
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

FDE upgrade failed

Stav	!
Součást	Šifrování dat
ID události systému Windows	1342
ID události aplikace Kaspersky Security Center	0000053e
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

Stav	!
Součást	Šifrování dat
ID události systému Windows	1344
ID události aplikace Kaspersky Security Center	00000540
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

Stav	!
Součást	Endpoint Sensor
ID události systému Windows	2100
ID události aplikace Kaspersky Security Center	00000834
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Failed to delete object

Stav	!
Součást	Sandbox
ID události systému Windows	2252
ID události aplikace Kaspersky Security Center	000008cc
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object not quarantined (Sandbox)

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2603
ID události aplikace Kaspersky Security Center	00000a2b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

An internal error occurred

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2607
ID události aplikace Kaspersky Security Center	00000a2f
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Invalid Sandbox server certificate

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2613
ID události aplikace Kaspersky Security Center	00000a35
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The Sandbox node is unavailable

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2614
ID události aplikace Kaspersky Security Center	00000a36
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Failed to process the object in Sandbox

Stav	ⓘ

Součást	Sandbox
ID události systému Windows	2617
ID události aplikace Kaspersky Security Center	00000a39
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Maximum load to Sandbox is exceeded

Stav	!
Součást	Sandbox
ID události systému Windows	2618
ID události aplikace Kaspersky Security Center	00000a3a
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

IOC found

Stav	!
Součást	Endpoint Detection and Response
ID události systému Windows	2651
ID události aplikace Kaspersky Security Center	00000a5b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Sandbox license verification failed

Stav	!
Součást	Sandbox
ID události systému Windows	2620
ID události aplikace Kaspersky Security Center	00000a3c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Odeslání úlohy kontroly do služby Sandbox se nezdařilo

Stav	!
Součást	Sandbox
ID události systému Windows	2623
ID události aplikace Kaspersky Security Center	00000a3e
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Při vytváření úlohy součásti Sandbox došlo k chybě

Stav	⊗
Součást	Sandbox
ID události systému Windows	2621
ID události aplikace Kaspersky Security Center	00000a3d
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object startup blocked

Stav	⊗
Součást	Endpoint Detection and Response
ID události systému Windows	2553
ID události aplikace Kaspersky Security Center	000009f9
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process startup blocked

Stav	⊗
Součást	Endpoint Detection and Response
ID události systému Windows	2551
ID události aplikace Kaspersky Security Center	000009f7
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Script execution blocked

Stav	⊗
Součást	Endpoint Detection and Response
ID události systému Windows	2559
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object not quarantined (Endpoint Detection and Response)

Stav	⊗
Součást	Endpoint Detection and Response
ID události systému Windows	2556
ID události aplikace Kaspersky Security Center	000009fc

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process startup is not blocked

Stav	!
Součást	Endpoint Detection and Response
ID události systému Windows	2561
ID události aplikace Kaspersky Security Center	00000a01
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object is not blocked

Stav	!
Součást	Endpoint Detection and Response
ID události systému Windows	2562
ID události aplikace Kaspersky Security Center	00000a02
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Script execution is not blocked

Stav	!
Součást	Endpoint Detection and Response
ID události systému Windows	2563
ID události aplikace Kaspersky Security Center	00000a03
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error changing application components

Stav	!
Součást	Audit systému
ID události systému Windows	1401
ID události aplikace Kaspersky Security Center	00000579
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

There are patterns of a possible brute-force attack in the system

Stav	!
Součást	Kontrola protokolu
ID události systému Windows	2800
ID události aplikace Kaspersky Security Center	00000af0
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

There are patterns of a possible Windows Event Log abuse

Stav	!
Součást	Kontrola protokolu
ID události systému Windows	2801
ID události aplikace Kaspersky Security Center	00000af1
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Atypical actions detected on behalf of a new service installed

Stav	!
Součást	Kontrola protokolu
ID události systému Windows	2802
ID události aplikace Kaspersky Security Center	00000af2
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Atypical logon that uses explicit credentials detected

Stav	!
Součást	Kontrola protokolu
ID události systému Windows	2803
ID události aplikace Kaspersky Security Center	00000af3
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

Stav	!
Součást	Kontrola protokolu
ID události systému Windows	2804
ID události aplikace Kaspersky Security Center	00000af4
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Suspicious changes detected in the privileged built-in Administrators group

Stav	ⓘ
Součást	Kontrola protokolu
ID události systému Windows	2805
ID události aplikace Kaspersky Security Center	00000af5
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

There is an atypical activity detected during a network logon session

Stav	ⓘ
Součást	Kontrola protokolu
ID události systému Windows	2806
ID události aplikace Kaspersky Security Center	00000af6
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Log Inspection rule triggered

Stav	ⓘ
Součást	Kontrola protokolu
ID události systému Windows	2807
ID události aplikace Kaspersky Security Center	00000af7
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Atypical event occurs too often. Event aggregation started

Stav	ⓘ
Součást	Kontrola protokolu
ID události systému Windows	2808
ID události aplikace Kaspersky Security Center	00000af8
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Report on an atypical event for the aggregation period

Stav	ⓘ

Součást	Kontrola protokolu
ID události systému Windows	2809
ID události aplikace Kaspersky Security Center	00000af9
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error connecting to the EDR Expert server

Stav	⊗
Součást	Endpoint Detection and Response Expert (on-premise)
ID události systému Windows	2850
ID události aplikace Kaspersky Security Center	00000b22
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Invalid certificate of the EDR Expert server

Stav	⊗
Součást	Endpoint Detection and Response Expert (on-premise)
ID události systému Windows	2851
ID události aplikace Kaspersky Security Center	00000b23
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Invalid certificate of the agent on the EDR Expert server

Stav	⊗
Součást	Endpoint Detection and Response Expert (on-premise)
ID události systému Windows	2852
ID události aplikace Kaspersky Security Center	00000b24
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Při připojování k serveru pro zpracování odpovědí EDR Expert došlo k chybě

Stav	⊗
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2858
ID události aplikace Kaspersky Security Center	00000b22
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát serveru pro zpracování odpovědí EDR Expert

Stav	⚠
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2859
ID události aplikace Kaspersky Security Center	00000b23
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát agenta na serveru pro zpracování odpovědí EDR Expert

Stav	⚠
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2860
ID události aplikace Kaspersky Security Center	00000b24
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chyba připojení k serveru pro shromažďování telemetrie EDR Expert

Stav	⚠
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2854
ID události aplikace Kaspersky Security Center	00000b22
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát serveru pro shromažďování telemetrie EDR Expert

Stav	⚠
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2855
ID události aplikace Kaspersky Security Center	00000b23
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát agenta na serveru pro shromažďování telemetrie EDR Expert

Stav	
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	2856
ID události aplikace Kaspersky Security Center	00000b24
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chyba připojení k serveru NDR

Stav	
Součást	Network Detection and Response (KATA)
ID události systému Windows	3080
ID události aplikace Kaspersky Security Center	00000c08
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát serveru NDR

Stav	
Součást	Network Detection and Response (KATA)
ID události systému Windows	3081
ID události aplikace Kaspersky Security Center	00000c09
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát agenta na serveru NDR

Stav	
Součást	Network Detection and Response (KATA)
ID události systému Windows	3082
ID události aplikace Kaspersky Security Center	00000c0a
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Vaše zařízení je připojeno k nedůvěryhodnému serveru pro správu. Kontaktujte správce

Stav	
Součást	Ochrana připojení k serveru pro správu
ID události systému Windows	3301
ID události aplikace Kaspersky Security Center	00000ce5

Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File or folder change was detected

Stav	ⓘ / ⚠ / ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2950
ID události aplikace Kaspersky Security Center	00000b86
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected.*

Object changes too often. Event aggregation started

Stav	ⓘ / ⚠ / ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2955
ID události aplikace Kaspersky Security Center	00000b8b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Report on object modification for the aggregation period

Stav	ⓘ / ⚠ / ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2956
ID události aplikace Kaspersky Security Center	00000b8c
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected.*

Monitoring scope includes incorrect objects

Stav	!
Součást	Monitorování integrity systému
ID události systému Windows	2953
ID události aplikace Kaspersky Security Center	00000b89
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Registry change was detected

Stav	i / ⚠ / !
Součást	Monitorování integrity systému
ID události systému Windows	2951
ID události aplikace Kaspersky Security Center	00000b87
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Device connection / disconnection is detected

Stav	i / ⚠ / !
Součást	Monitorování integrity systému
ID události systému Windows	2952
ID události aplikace Kaspersky Security Center	00000b88
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Součástí monitorování jsou nesprávné objekty

Stav	i / ⚠ / !
Součást	Monitorování integrity systému
ID události systému Windows	2903
ID události aplikace Kaspersky Security Center	00000b89
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Attempts to perform the restricted operations with the object is too many. Event aggregation started

Stav	!
Součást	Monitorování integrity systému
ID události systému Windows	2963
ID události aplikace Kaspersky Security Center	00000b93
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

An operation with the files of the monitoring scope was blocked

Stav	!
Součást	Monitorování integrity systému
ID události systému Windows	2959
ID události aplikace Kaspersky Security Center	00000b8f
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Registry modification blocked

Stav	!
Součást	Monitorování integrity systému
ID události systému Windows	2960
ID události aplikace Kaspersky Security Center	00000b90
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Processing error

Stav	⚠
Součást	Monitorování integrity systému
ID události systému Windows	2954
ID události aplikace Kaspersky Security Center	00000b8a
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	⚠
Součást	Monitorování integrity systému
ID události systému Windows	2964
ID události aplikace Kaspersky Security Center	00000b94
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	⚠
Součást	Kontrola aplikací
ID události systému Windows	711
ID události aplikace Kaspersky Security Center	000002c7
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	⚠
Součást	Kontrola zařízení
ID události systému Windows	810
ID události aplikace Kaspersky Security Center	0000032a
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	⚠

Součást	Kontrola webu
ID události systému Windows	757
ID události aplikace Kaspersky Security Center	000002f5
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	ⓘ
Součást	Adaptivní kontrola anomálií
ID události systému Windows	504
ID události aplikace Kaspersky Security Center	000001f8
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

Stav	ⓘ
Součást	Kontrola protokolu
ID události systému Windows	2810
ID události aplikace Kaspersky Security Center	00000afa
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Unable to connect to the Integration Server for more than 6 hours. Check Integration Server status and network settings

Stav	ⓘ
Součást	Light Agent
ID události systému Windows	3103
ID události aplikace Kaspersky Security Center	00000c1f
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

SVM is unavailable

Stav	ⓘ
Součást	Light Agent
ID události systému Windows	3151
ID události aplikace Kaspersky Security Center	00000c4f

Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Malicious object detected. Advanced Disinfection should be started on a virtual machine template

Stav	ⓘ
Součást	Light Agent
ID události systému Windows	3182
ID události aplikace Kaspersky Security Center	00000c6e
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Bylo zablokováno síťové připojení navázané přes zastaralý protokol

Stav	ⓘ
Součást	Ochrana
ID události systému Windows	75
ID události aplikace Kaspersky Security Center	0000004b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chyba připojení k serveru KUMA

Stav	ⓘ
Součást	Integrace KUMA
ID události systému Windows	2854
ID události aplikace Kaspersky Security Center	00000b26
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát serveru KUMA

Stav	ⓘ
Součást	Integrace KUMA
ID události systému Windows	2855
ID události aplikace Kaspersky Security Center	00000b27
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Neplatný certifikát agenta na serveru KUMA

Stav	⊗
Součást	Integrace KUMA
ID události systému Windows	2856
ID události aplikace Kaspersky Security Center	00000b28
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chyby funkcí

Rozbalit vše | Sbalit vše

Task cannot be performed

Stav	⊗
Součást	Audit systému
ID události systému Windows	212
ID události aplikace Kaspersky Security Center	000000d4
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Invalid task settings. Settings not applied

Stav	⊗
Součást	Audit systému
ID události systému Windows	707
ID události aplikace Kaspersky Security Center	000002c3
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Varování

Rozbalit vše | Sbalit vše

Application crashed during previous session

Stav	⚠
Součást	Audit systému
ID události systému Windows	237
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

License expires soon

Stav	⚠
Součást	Audit systému
ID události systému Windows	204
ID události aplikace Kaspersky Security Center	000000cc
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Databases are out of date

Stav	⚠
Součást	Audit systému
ID události systému Windows	208
ID události aplikace Kaspersky Security Center	000000d0
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Automatic updates are disabled

Stav	⚠
Součást	Audit systému
ID události systému Windows	210
ID události aplikace Kaspersky Security Center	000000d2
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Self-Defense is disabled

Stav	⚠
Součást	Audit systému
ID události systému Windows	211
ID události aplikace Kaspersky Security Center	000000d3
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Protection components are disabled

Stav	⚠
Součást	Audit systému
ID události systému Windows	214
ID události aplikace Kaspersky Security Center	000000d6
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Computer is running in safe mode

Stav	⚠
Součást	Audit systému
ID události systému Windows	215
ID události aplikace Kaspersky Security Center	000000d7
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

There are unprocessed files

Stav	⚠
Součást	Audit systému
ID události systému Windows	216
ID události aplikace Kaspersky Security Center	000000d8
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Group policy applied

Stav	⚠
Součást	Audit systému
ID události systému Windows	219
ID události aplikace Kaspersky Security Center	000000db
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Task stopped

Stav	⚠
Součást	Audit systému
ID události systému Windows	222
ID události aplikace Kaspersky Security Center	000000de
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Quit and reopen the application to complete updating

Stav	⚠

Součást	Audit systému
ID události systému Windows	224
ID události aplikace Kaspersky Security Center	0000057b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Computer restart required

Stav	⚠
Součást	Audit systému
ID události systému Windows	225
ID události aplikace Kaspersky Security Center	000000e1
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The license allows the use of components that have not been installed

Stav	⚠
Součást	Audit systému
ID události systému Windows	226
ID události aplikace Kaspersky Security Center	000000e2
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Advanced Disinfection started

Stav	⚠
Součást	Audit systému
ID události systému Windows	232
ID události aplikace Kaspersky Security Center	000000e8
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Advanced Disinfection completed

Stav	⚠
Součást	Audit systému
ID události systému Windows	233
ID události aplikace Kaspersky Security Center	000000e9
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Incorrect reserve key

Stav	⚠
Součást	Audit systému
ID události systému Windows	`230`
ID události aplikace Kaspersky Security Center	`000000e6`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Subscription expires soon

Stav	⚠
Součást	Audit systému
ID události systému Windows	`240`
ID události aplikace Kaspersky Security Center	`000000f0`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Blokováno

Stav	⚠
Součást	Detekce chování Anti-Cryptor Prevence zneužití Ochrana před webovými hrozbami
ID události systému Windows	`331`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. Když je zjištěno externí šifrování sdílených složek, aplikace ukazuje cestu k cílovému souboru. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

The operating system settings do not allow to control access to Wi-Fi networks

Stav	⚠
Součást	Kontrola zařízení
ID události systému Windows	249
ID události aplikace Kaspersky Security Center	000000f9
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Object not restored from Backup

Stav	⚠
Součást	Audit systému
ID události systému Windows	336
ID události aplikace Kaspersky Security Center	00000150
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Suspicious network activity detected

Stav	⚠
Součást	Audit systému
ID události systému Windows	2001
ID události aplikace Kaspersky Security Center	000007d1
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Encrypted connection terminated

Stav	⚠
Součást	Audit systému
ID události systému Windows	250
ID události aplikace Kaspersky Security Center	000007d3
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Participation in KSN disabled

Stav	⚠
Součást	Audit systému
ID události systému Windows	2021
ID události aplikace Kaspersky Security Center	000007e5
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Processing of some OS functions is disabled

Stav	⚠
Součást	Audit systému
ID události systému Windows	245
ID události aplikace Kaspersky Security Center	000000f5
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Quarantine storage is almost out of space

Stav	⚠
Součást	Audit systému
ID události systému Windows	344
ID události aplikace Kaspersky Security Center	00000158
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network connection blocked

Stav	⚠
Součást	Audit systému
ID události systému Windows	809
ID události aplikace Kaspersky Security Center	00000abe
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Cannot create a backup copy

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Ochrana AMSI Kontrola malwaru
ID události systému Windows	314

ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_REPORTED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Stav	⚠
Součást	Ochrana před souborovými hrozbami Detekce chování Anti-Cryptor Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	`310`
ID události aplikace Kaspersky Security Center	`00000136`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object encrypted

Stav	⚠
Součást	Prevence narušení hostitele
ID události systému Windows	`320`
ID události aplikace Kaspersky Security Center	`00000140`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Object corrupted

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI

	Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	`321`
ID události aplikace Kaspersky Security Center	`00000141`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Ochrana AMSI Detekce chování Anti-Cryptor Anti-Cryptor Kontrola malwaru
ID události systému Windows	`303`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`).
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Ochrana AMSI Detekce chování Anti-Cryptor Anti-Cryptor Kontrola malwaru
ID události systému Windows	`303`
ID události aplikace Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`).

Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object deleted

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Prevence zneužití Detekce chování Anti-Cryptor Kontrola malwaru
ID události systému Windows	`307`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_DELETED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object disinfected

Stav	⚠
Součást	Ochrana před souborovými hrozbami Ochrana před hrozbami v poště Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	`306`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_CURED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`).

	• `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object will be disinfected on restart

Stav	⚠
Součást	Prevence narušení hostitele Ochrana před souborovými hrozbami Kontrola malwaru
ID události systému Windows	324
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Object will be deleted on restart

Stav	⚠
Součást	Detekce chování Anti-Cryptor Prevence zneužití Prevence narušení hostitele Ochrana před souborovými hrozbami Kontrola malwaru
ID události systému Windows	323
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Object deleted according to settings

Stav	⚠
Součást	Ochrana před hrozbami v poště
ID události systému Windows	342
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Rollback completed

Stav	⚠
Součást	Ochrana před souborovými hrozbami Detekce chování Anti-Cryptor Prevence zneužití Kontrola malwaru
ID události systému Windows	`455`
ID události aplikace Kaspersky Security Center	`000001c7`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object download was blocked

Stav	⚠
Součást	Ochrana před webovými hrozbami
ID události systému Windows	`341`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Keyboard authorization error

Stav	⚠
Součást	Ochrana před útoky BadUSB
ID události systému Windows	`2052`
ID události aplikace Kaspersky Security Center	`00000804`
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The object scan result has been sent to a third-party application

Stav	⚠
Součást	Ochrana AMSI
ID události systému Windows	`1512`
ID události aplikace Kaspersky Security Center	`GNRL_EV_OBJECT_REPORTED`
Parametry události	• `GNRL_EA_PARAM_1` je hash objektu (SHA256). • `GNRL_EA_PARAM_2` je název objektu. • `GNRL_EA_PARAM_5` je název hrozby dle klasifikace společnosti Kaspersky, např. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_8` je typ hrozby (`type`). • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná službou Kaspersky Private Security Network (`blacklist`): `true` nebo `false`. Verze EDR. Identifikátor hrozby v EDR. MD5 hash objektu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Task settings applied successfully

Stav	⚠
Součást	Kontrola aplikací
ID události systému Windows	`708`
ID události aplikace Kaspersky Security Center	`000002c4`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Warning about undesirable content (local bases)

Stav	⚠
Součást	Kontrola webu
ID události systému Windows	`708`
ID události aplikace Kaspersky Security Center	`GNRL_EV_WEB_URL_WARNING`
Parametry události	• `GNRL_EA_PARAM_1` je URL.

	• GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je název pravidla součásti Kontrola webu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Warning about undesirable content (KSN)

Stav	⚠
Součást	Kontrola webu
ID události systému Windows	708
ID události aplikace Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Parametry události	• GNRL_EA_PARAM_1 je URL. • GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je název pravidla součásti Kontrola webu.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Undesirable content was accessed after a warning

Stav	⚠
Součást	Kontrola webu
ID události systému Windows	754
ID události aplikace Kaspersky Security Center	000002f2
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Temporary access to the device activated

Stav	⚠
Součást	Kontrola zařízení
ID události systému Windows	803
ID události aplikace Kaspersky Security Center	000002f2
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Operation canceled by the user

Stav	⚠
Součást	Aktualizace

ID události systému Windows	1016
ID události aplikace Kaspersky Security Center	000003f8
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

User has opted out of the encryption policy

Stav	⚠
Součást	Šifrování dat
ID události systému Windows	1306
ID události aplikace Kaspersky Security Center	0000051a
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Interrupted applying file encryption / decryption rules

Stav	⚠
Součást	Šifrování dat
ID události systému Windows	903
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File encryption / decryption interrupted

Stav	⚠
Součást	Šifrování dat
ID události systému Windows	914
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption interrupted

Stav	⚠
Součást	Šifrování dat
ID události systému Windows	1303
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

Stav	⚠
Součást	Šifrování dat
ID události systému Windows	1345
ID události aplikace Kaspersky Security Center	00000541
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Module signature check failed

Stav	⚠
Součást	Kontrola integrity systému
ID události systému Windows	2002
ID události aplikace Kaspersky Security Center	000007d2
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application startup was blocked

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2105
ID události aplikace Kaspersky Security Center	00000839
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Document opening was blocked

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2106
ID události aplikace Kaspersky Security Center	0000083a
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Stav	⚠

Součást	Endpoint Sensor
ID události systému Windows	2112
ID události aplikace Kaspersky Security Center	00000840
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2113
ID události aplikace Kaspersky Security Center	00000841
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2111
ID události aplikace Kaspersky Security Center	0000083f
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2110
ID události aplikace Kaspersky Security Center	0000083e
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by the administrator

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2109
ID události aplikace Kaspersky Security Center	0000083d

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network activity of all third-party applications is blocked

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2107
ID události aplikace Kaspersky Security Center	0000083b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network activity of all third-party applications is unblocked

Stav	⚠
Součást	Endpoint Sensor
ID události systému Windows	2108
ID události aplikace Kaspersky Security Center	0000083c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object will be deleted after restart (Sandbox)

Stav	⚠
Součást	Sandbox
ID události systému Windows	2605
ID události aplikace Kaspersky Security Center	00000a2d
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Total size of scan tasks exceeded the limit

Stav	⚠
Součást	Sandbox
ID události systému Windows	2612
ID události aplikace Kaspersky Security Center	00000a34
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object startup allowed, event logged

Stav	⚠
Součást	Endpoint Detection and Response
ID události systému Windows	2553
ID události aplikace Kaspersky Security Center	000009fa
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Process startup allowed, event logged

Stav	⚠
Součást	Endpoint Detection and Response
ID události systému Windows	2554
ID události aplikace Kaspersky Security Center	000009f8
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object will be deleted after restart (Endpoint Detection and Response)

Stav	⚠
Součást	Endpoint Detection and Response
ID události systému Windows	2558
ID události aplikace Kaspersky Security Center	000009fe
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network isolation

Stav	⚠
Součást	Endpoint Detection and Response
ID události systému Windows	2700
ID události aplikace Kaspersky Security Center	00000a8c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Termination of network isolation

Stav	⚠

Součást	Endpoint Detection and Response
ID události systému Windows	2701
ID události aplikace Kaspersky Security Center	00000a8d
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Restart required to complete the task

Stav	⚠
Součást	Audit systému
ID události systému Windows	225
ID události aplikace Kaspersky Security Center	0000057b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application startup blockage message to administrator

Stav	⚠
Součást	Kontrola aplikací
ID události systému Windows	503
ID události aplikace Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Parametry události	• GNRL_EA_DESCRIPTION je zpráva uživateli. • GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_6 je název spustitelného souboru aplikace (například chrome.exe). • GNRL_EA_PARAM_7 je cesta ke spustitelnému souboru. • GNRL_EA_PARAM_8 je hash objektu (SHA256). • GNRL_EA_PARAM_9 je verze aplikace, kterou se uživatel pokouší spustit.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Device access blockage message to administrator

Stav	⚠
Součást	Kontrola zařízení
ID události systému Windows	804
ID události aplikace Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Parametry události	• c_er_descr je zpráva uživateli. • GNRL_EA_PARAM_1 je ID hardwaru (HWID). • GNRL_EA_PARAM_2 je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Web page access blockage message to administrator

Stav	⚠
Součást	Kontrola webu
ID události systému Windows	755
ID události aplikace Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
Parametry události	• GNRL_EA_DESCRIPTION je zpráva uživateli. • GNRL_EA_PARAM_1 je URL. • GNRL_EA_PARAM_2 je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Device connection blocked

Stav	⚠
Součást	Kontrola zařízení
ID události systému Windows	807
ID události aplikace Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
Parametry události	• GNRL_EA_PARAM_1 je ID hardwaru (HWID). • GNRL_EA_PARAM_2 je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application activity blockage message to administrator

Stav	⚠
Součást	Monitor integrity souborů
ID události systému Windows	2901
ID události aplikace Kaspersky Security Center	00000b55
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Stav	⚠
Součást	Monitor integrity souborů
ID události systému Windows	2900
ID události aplikace Kaspersky Security Center	00000b54

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Stav	⚠
Součást	Adaptivní kontrola anomálií
ID události systému Windows	`503`
ID události aplikace Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Parametry události	• `GNRL_EA_DESCRIPTION` je zpráva uživateli. • `GNRL_EA_PARAM_1` je název pravidla součásti Adaptivní kontrola anomálií. • `GNRL_EA_PARAM_2` je ID heuristického pravidla. • `GNRL_EA_PARAM_3` je jméno uživatele relace. • `GNRL_EA_PARAM_4` je zdrojový proces. • `GNRL_EA_PARAM_5` je zdrojový objekt. • `GNRL_EA_PARAM_6` je cílový proces. • `GNRL_EA_PARAM_7` je cílový objekt. • `GNRL_EA_PARAM_8` jsou další informace o detekovaném objektu: Hodnoty hash zdrojového procesu/objektu a cílového procesu/objektu. Proces zablokován (`verdict_type`): `true` nebo `false`. ID zabezpečení uživatele (SID).
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Starting the cloud service client application is blocked

Stav	⚠
Součást	Cloud Discovery
ID události systému Windows	`2212`
ID události aplikace Kaspersky Security Center	`000008a4`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Access to the cloud service is blocked

Stav	⚠
Součást	Cloud Discovery
ID události systému Windows	`2213`
ID události aplikace Kaspersky Security Center	`000008a5`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File or folder change was detected

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2950
ID události aplikace Kaspersky Security Center	00000b86
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Object changes too often. Event aggregation started

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2955
ID události aplikace Kaspersky Security Center	00000b8b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Report on object modification for the aggregation period

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2956
ID události aplikace Kaspersky Security Center	00000b8c
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Registry change was detected

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2951

ID události aplikace Kaspersky Security Center	00000b87
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Device connection / disconnection is detected

Stav	ⓘ / ⚠ / ⓔ
Součást	Monitorování integrity systému
ID události systému Windows	2952
ID události aplikace Kaspersky Security Center	00000b88
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Součástí monitorování jsou nesprávné objekty

Stav	ⓘ / ⚠ / ⓔ
Součást	Monitorování integrity systému
ID události systému Windows	2903
ID události aplikace Kaspersky Security Center	00000b89
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

The prohibited operation was allowed in test mode

Stav	⚠
Součást	Monitorování integrity systému
ID události systému Windows	2961
ID události aplikace Kaspersky Security Center	00000b91
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Nelze se připojit k integračnímu serveru déle než 30 minut. Zkontrolujte stav integračního serveru a nastavení sítě

Stav	⚠
Součást	Light Agent
ID události systému Windows	3102
ID události aplikace Kaspersky Security Center	00000c1e
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Nelze se připojit k integračnímu serveru. Zkontrolujte stav integračního serveru a nastavení sítě

Stav	⚠
Součást	Light Agent
ID události systému Windows	3101
ID události aplikace Kaspersky Security Center	00000c1d
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Šablonu virtuálního počítače je třeba aktualizovat

Stav	⚠
Součást	Light Agent
ID události systému Windows	3181
ID události aplikace Kaspersky Security Center	00000c6d
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The Standard license is terminated. The application is running under the Enterprise license

Stav	⚠
Součást	Light Agent
ID události systému Windows	3171
ID události aplikace Kaspersky Security Center	00000c64
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Informační zpráva

Application started

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	235
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Application stopped

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	236
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Self-Defense restricted access to the protected resource

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	213
ID události aplikace Kaspersky Security Center	000000d5
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Report cleared

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	217
ID události aplikace Kaspersky Security Center	000000d9
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Group policy disabled

Stav	
Součást	Audit systému
ID události systému Windows	220
ID události aplikace Kaspersky Security Center	000000dc
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Application settings changed

Stav	
Součást	Audit systému
ID události systému Windows	218
ID události aplikace Kaspersky Security Center	000000da
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Task started

Stav	
Součást	Audit systému
ID události systému Windows	221
ID události aplikace Kaspersky Security Center	000000dd
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Task completed

Stav	
Součást	Audit systému
ID události systému Windows	223
ID události aplikace Kaspersky Security Center	000000df
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

All application components that are defined by the license have been installed and run in normal mode

Stav	
Součást	Audit systému
ID události systému Windows	227

ID události aplikace Kaspersky Security Center	000000e3
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Subscription settings have changed

Stav	
Součást	Audit systému
ID události systému Windows	238
ID události aplikace Kaspersky Security Center	000000ee
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Subscription has been renewed

Stav	
Součást	Audit systému
ID události systému Windows	239
ID události aplikace Kaspersky Security Center	000000ef
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object restored from Backup

Stav	
Součást	Audit systému
ID události systému Windows	335
ID události aplikace Kaspersky Security Center	0000014f
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

User name and password input

Stav	
Součást	Audit systému
ID události systému Windows	2000
ID události aplikace Kaspersky Security Center	000007d0
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Participation in KSN enabled

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	2020
ID události aplikace Kaspersky Security Center	000007e4
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

KSN servers available

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	2022
ID události aplikace Kaspersky Security Center	000007e6
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	2024
ID události aplikace Kaspersky Security Center	000007e8
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object restored from Quarantine

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	345
ID události aplikace Kaspersky Security Center	00000159
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object deleted from Quarantine

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	347
ID události aplikace Kaspersky Security Center	0000015b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

A backup copy of the object was created

Stav	ⓘ
Součást	Ochrana před souborovými hrozbami Ochrana před hrozbami v poště Detekce chování Anti-Cryptor Prevence narušení hostitele Sandbox Kontrola malwaru
ID události systému Windows	308
ID události aplikace Kaspersky Security Center	00000134
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Overwritten by a copy that was disinfected earlier

Stav	ⓘ
Součást	Ochrana před souborovými hrozbami Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	327
ID události aplikace Kaspersky Security Center	00000147
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Password-protected archive detected

Stav	ⓘ
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	322
ID události aplikace Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Parametry události	• GNRL_EA_PARAM_2 je název objektu. • GNRL_EA_PARAM_3 je datum vytvoření objektu (volitelné).

	• `GNRL_EA_PARAM_7` je jméno uživatele relace. • `GNRL_EA_PARAM_9` jsou další informace o detekovaném objektu: Součást aplikace (`engine`). Technologie detekce hrozeb (`method`). Hrozba zjištěná privátní KSN (seznam zakázaných položek): true nebo false.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Information about detected object

Stav	ⓘ
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	`332`
ID události aplikace Kaspersky Security Center	`0000014c`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The object is in the Kaspersky Private Security Network allowlist

Stav	ⓘ
Součást	Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Prevence narušení hostitele Kontrola malwaru
ID události systému Windows	`340`
ID události aplikace Kaspersky Security Center	`00000154`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object renamed

Stav	ⓘ
Součást	Ochrana před hrozbami v poště Prevence zneužití Detekce chování Anti-Cryptor Kontrola malwaru
ID události systému Windows	`329`

ID události aplikace Kaspersky Security Center	00000149
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object processed

Stav	ⓘ
Součást	Prevence narušení hostitele Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Kontrola malwaru
ID události systému Windows	301
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Object skipped

Stav	ⓘ
Součást	Prevence narušení hostitele Ochrana před souborovými hrozbami Ochrana AMSI Kontrola malwaru
ID události systému Windows	315
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Archive detected

Stav	ⓘ
Součást	Prevence narušení hostitele Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Kontrola malwaru
ID události systému Windows	318
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Packed object detected

Stav	
Součást	Prevence narušení hostitele Ochrana před souborovými hrozbami Ochrana před webovými hrozbami Ochrana před hrozbami v poště Ochrana AMSI Kontrola malwaru
ID události systému Windows	319
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Link processed

Stav	
Součást	Ochrana před webovými hrozbami
ID události systému Windows	361
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Application startup allowed

Stav	
Součást	Kontrola aplikací
ID události systému Windows	701
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Update source is selected

Stav	
Součást	Aktualizace
ID události systému Windows	1001
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Je vybrán proxy server

Stav	
Součást	Aktualizace
ID události systému Windows	1002
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

The link is in the Kaspersky Private Security Network allowlist

Stav	
Součást	Ochrana před webovými hrozbami
ID události systému Windows	370
ID události aplikace Kaspersky Security Center	00000172
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application placed in the trusted group

Stav	
Součást	Prevence narušení hostitele
ID události systému Windows	401
ID události aplikace Kaspersky Security Center	00000191
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application placed in restricted group

Stav	
Součást	Prevence narušení hostitele
ID události systému Windows	402
ID události aplikace Kaspersky Security Center	00000192
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Host Intrusion Prevention was triggered

Stav	
Součást	Prevence narušení hostitele
ID události systému Windows	403

ID události aplikace Kaspersky Security Center	00000193
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File restored

Stav	
Součást	Detekce chování Anti-Cryptor Prevence zneužití Prevence narušení hostitele
ID události systému Windows	457
ID události aplikace Kaspersky Security Center	000001c9
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Registry value restored

Stav	
Součást	Detekce chování Prevence zneužití
ID události systému Windows	458
ID události aplikace Kaspersky Security Center	000001ca
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Registry value deleted

Stav	
Součást	Detekce chování Prevence zneužití
ID události systému Windows	459
ID události aplikace Kaspersky Security Center	000001cb
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Process action skipped

Stav	
Součást	Adaptivní kontrola anomálií
ID události systému Windows	2201

ID události aplikace Kaspersky Security Center	`GNRL_EV_ADSEC_DETECT`
Parametry události	• `GNRL_EA_PARAM_1` je název pravidla součásti Adaptivní kontrola anomálií. • `GNRL_EA_PARAM_2` je ID heuristického pravidla. • `GNRL_EA_PARAM_3` je jméno uživatele relace. • `GNRL_EA_PARAM_4` je zdrojový proces. • `GNRL_EA_PARAM_5` je zdrojový objekt. • `GNRL_EA_PARAM_6` je cílový proces. • `GNRL_EA_PARAM_7` je cílový objekt. • `GNRL_EA_PARAM_8` jsou další informace o detekovaném objektu: Hodnoty hash zdrojového procesu/objektu a cílového procesu/objektu. Proces zablokován (`verdict_type`): `true` nebo `false`. ID zabezpečení uživatele (SID).
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Keyboard authorized

Stav	
Součást	Ochrana před útoky BadUSB
ID události systému Windows	`2050`
ID události aplikace Kaspersky Security Center	`00000802`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Network activity allowed

Stav	
Součást	Brána firewall
ID události systému Windows	`601`
ID události aplikace Kaspersky Security Center	`00000259`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Application startup prohibited in test mode

Stav	
Součást	Kontrola aplikací
ID události systému Windows	`703`
ID události aplikace Kaspersky Security Center	`GNRL_EV_APP_LAUNCH_TESTED_DENIED`

Parametry události	• GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je ručně vytvořený identifikátor kategorie. • GNRL_EA_PARAM_4 je identifikátor zabezpečení účtu (SID). • GNRL_EA_PARAM_5 jsou údaje o digitálním podpisu aplikace. • GNRL_EA_PARAM_6 je název spustitelného souboru aplikace (například chrome.exe). • GNRL_EA_PARAM_7 je cesta ke spustitelnému souboru. • GNRL_EA_PARAM_8 je hash objektu (SHA256). • GNRL_EA_PARAM_9 je verze aplikace, kterou se uživatel pokouší spustit.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application startup allowed in test mode

Stav	ⓘ
Součást	Kontrola aplikací
ID události systému Windows	704
ID události aplikace Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Parametry události	• GNRL_EA_PARAM_2 je jméno uživatele relace. • GNRL_EA_PARAM_3 je ručně vytvořený identifikátor kategorie. • GNRL_EA_PARAM_4 je identifikátor zabezpečení účtu (SID). • GNRL_EA_PARAM_5 jsou údaje o digitálním podpisu aplikace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

A page that is allowed was opened

Stav	ⓘ
Součást	Kontrola webu
ID události systému Windows	751
ID události aplikace Kaspersky Security Center	000002f4
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Operation with the device allowed

Stav	ⓘ
Součást	Kontrola zařízení
ID události systému Windows	801
ID události aplikace Kaspersky Security Center	00000321

Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File operation performed

Stav	
Součást	Kontrola zařízení
ID události systému Windows	`808`
ID události aplikace Kaspersky Security Center	`GNRL_EV_USB_FILE_OPERATION`
Parametry události	• `GNRL_EA_PARAM_1` je operace u souboru (zápis nebo odstranění). • `GNRL_EA_PARAM_2` je cesta k souboru. • `GNRL_EA_PARAM_3` je název zařízení. • `GNRL_EA_PARAM_4` je jméno uživatele relace. • `GNRL_EA_PARAM_5` je ID hardwaru (HWID).
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

No available updates

Stav	
Součást	Aktualizace
ID události systému Windows	`1020`
ID události aplikace Kaspersky Security Center	`000003fc`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Update distribution completed successfully

Stav	
Součást	Aktualizace
ID události systému Windows	`1022`
ID události aplikace Kaspersky Security Center	`000003fe`
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Downloading files

Stav	
Součást	Aktualizace

ID události systému Windows	1003
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File downloaded

Stav	
Součást	Aktualizace
ID události systému Windows	1004
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File installed

Stav	
Součást	Aktualizace
ID události systému Windows	1005
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File updated

Stav	
Součást	Aktualizace
ID události systému Windows	1006
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File rolled back due to update error

Stav	
Součást	Aktualizace
ID události systému Windows	1007
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Updating files

Stav	
Součást	Aktualizace
ID události systému Windows	1008
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Distributing updates

Stav	
Součást	Aktualizace
ID události systému Windows	1009
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Rolling back files

Stav	
Součást	Aktualizace
ID události systému Windows	1010
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Creating the list of files to download

Stav	
Součást	Aktualizace
ID události systému Windows	1013
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Downloading patches

Stav	
Součást	Aktualizace
ID události systému Windows	2150
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Installing patch

Stav	
Součást	Aktualizace
ID události systému Windows	2151
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Patch installed

Stav	
Součást	Aktualizace
ID události systému Windows	2152
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Rolling back patch

Stav	
Součást	Aktualizace
ID události systému Windows	2154
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Patch rolled back

Stav	
Součást	Aktualizace

ID události systému Windows	2155
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Started applying file encryption / decryption rules

Stav	
Součást	Šifrování dat
ID události systému Windows	901
ID události aplikace Kaspersky Security Center	00000385
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Finished applying file encryption / decryption rules

Stav	
Součást	Šifrování dat
ID události systému Windows	902
ID události aplikace Kaspersky Security Center	00000386
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Resumed applying file encryption / decryption rules

Stav	
Součást	Šifrování dat
ID události systému Windows	905
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File encryption / decryption started

Stav	
Součást	Šifrování dat
ID události systému Windows	910
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File encryption / decryption completed

Stav	
Součást	Šifrování dat
ID události systému Windows	911
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

File has not been encrypted because it is an exclusion

Stav	
Součást	Šifrování dat
ID události systému Windows	913
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Portable mode enabled

Stav	
Součást	Šifrování dat
ID události systému Windows	950
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Portable mode disabled

Stav	
Součást	Šifrování dat
ID události systému Windows	952
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption started

Stav	
Součást	Šifrování dat
ID události systému Windows	1301
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption completed

Stav	
Součást	Šifrování dat
ID události systému Windows	1302
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption resumed

Stav	
Součást	Šifrování dat
ID události systému Windows	1304
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device is not encrypted

Stav	
Součást	Šifrování dat
ID události systému Windows	1307
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption process has been switched to active mode

Stav	
Součást	Šifrování dat

ID události systému Windows	1308
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Device encryption / decryption process has been switched to passive mode

Stav	
Součást	Šifrování dat
ID události systému Windows	1309
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Encryption module loaded

Stav	
Součást	Šifrování dat
ID události systému Windows	1310
ID události aplikace Kaspersky Security Center	0000051e
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

New Authentication Agent account created

Stav	
Součást	Šifrování dat
ID události systému Windows	1330
ID události aplikace Kaspersky Security Center	00000532
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Authentication Agent account deleted

Stav	
Součást	Šifrování dat
ID události systému Windows	1331
ID události aplikace Kaspersky Security Center	00000533
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Authentication Agent account password changed

Stav	
Součást	Šifrování dat
ID události systému Windows	1332
ID události aplikace Kaspersky Security Center	00000534
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Successful Authentication Agent login

Stav	
Součást	Šifrování dat
ID události systému Windows	1333
ID události aplikace Kaspersky Security Center	00000535
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Failed Authentication Agent login attempt

Stav	
Součást	Šifrování dat
ID události systému Windows	1334
ID události aplikace Kaspersky Security Center	00000536
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

Stav	
Součást	Šifrování dat
ID události systému Windows	1335
ID události aplikace Kaspersky Security Center	00000537
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

Stav	
Součást	Šifrování dat
ID události systému Windows	1336
ID události aplikace Kaspersky Security Center	00000538
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Account was not added. This account already exists

Stav	
Součást	Šifrování dat
ID události systému Windows	1337
ID události aplikace Kaspersky Security Center	00000539
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Account was not modified. This account does not exist

Stav	
Součást	Šifrování dat
ID události systému Windows	1338
ID události aplikace Kaspersky Security Center	0000053a
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Account was not deleted. This account does not exist

Stav	
Součást	Šifrování dat
ID události systému Windows	1339
ID události aplikace Kaspersky Security Center	0000053b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

FDE upgrade successful

Stav	
Součást	Šifrování dat

ID události systému Windows	1341
ID události aplikace Kaspersky Security Center	0000053d
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

FDE upgrade rollback successful

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1343
ID události aplikace Kaspersky Security Center	0000053f
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1346
ID události aplikace Kaspersky Security Center	00000542
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

BitLocker recovery key was changed

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1370
ID události aplikace Kaspersky Security Center	0000055a
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

BitLocker password / PIN was changed

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1371
ID události aplikace Kaspersky Security Center	0000055b
Protokol událostí systému Windows (výchozí)	✓

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

BitLocker recovery key was saved to a removable drive

Stav	ⓘ
Součást	Šifrování dat
ID události systému Windows	1372
ID události aplikace Kaspersky Security Center	0000055c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

Stav	ⓘ
Součást	Endpoint Sensor
ID události systému Windows	2103
ID události aplikace Kaspersky Security Center	00000837
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Endpoint Sensor connected to server

Stav	ⓘ
Součást	Endpoint Sensor
ID události systému Windows	2101
ID události aplikace Kaspersky Security Center	00000835
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

Stav	ⓘ
Součást	Endpoint Sensor
ID události systému Windows	2102
ID události aplikace Kaspersky Security Center	00000836
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

Stav	
Součást	Endpoint Sensor
ID události systému Windows	2104
ID události aplikace Kaspersky Security Center	00000838
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object deleted

Stav	
Součást	Výmaz dat
ID události systému Windows	2251
ID události aplikace Kaspersky Security Center	000008cb
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Wipe task statistics

Stav	
Součást	Endpoint Detection and Response Expert (on-premise)
ID události systému Windows	2853
ID události aplikace Kaspersky Security Center	00000b25
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Stav	
Součást	Výmaz dat
ID události systému Windows	2253
ID události aplikace Kaspersky Security Center	000008cd
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object quarantined (Sandbox)

Stav	
Součást	Sandbox
ID události systému Windows	2602
ID události aplikace Kaspersky Security Center	00000a2a

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object deleted (Sandbox)

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2604
ID události aplikace Kaspersky Security Center	00000a2c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

IOC Scan started

Stav	ⓘ
Součást	Endpoint Detection and Response
ID události systému Windows	2652
ID události aplikace Kaspersky Security Center	00000a5c
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

IOC Scan completed

Stav	ⓘ
Součást	Endpoint Detection and Response
ID události systému Windows	2653
ID události aplikace Kaspersky Security Center	00000a5d
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object quarantined (Endpoint Detection and Response)

Stav	ⓘ
Součást	Endpoint Detection and Response
ID události systému Windows	2555
ID události aplikace Kaspersky Security Center	000009fb
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Object deleted (Endpoint Detection and Response)

Stav	
Součást	Endpoint Detection and Response
ID události systému Windows	2557
ID události aplikace Kaspersky Security Center	000009fd
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Application components successfully changed

Stav	
Součást	Audit systému
ID události systému Windows	1402
ID události aplikace Kaspersky Security Center	0000057a
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Stav	
Součást	Sandbox
ID události systému Windows	2606
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Stav	
Součást	Sandbox
ID události systému Windows	2609
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Stav	
Součást	Sandbox
ID události systému Windows	2610
ID události aplikace Kaspersky Security Center	–

Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Stav	ⓘ
Součást	Sandbox
ID události systému Windows	2616
ID události aplikace Kaspersky Security Center	–
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	–

Server pro správu, k němuž je zařízení připojeno, je nastaven jako důvěryhodný

Stav	ⓘ
Součást	Ochrana připojení k serveru pro správu
ID události systému Windows	3300
ID události aplikace Kaspersky Security Center	00000ce4
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Vaše zařízení je připojeno k novému důvěryhodnému serveru pro správu

Stav	ⓘ
Součást	Ochrana připojení k serveru pro správu
ID události systému Windows	3302
ID události aplikace Kaspersky Security Center	00000ce6
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Server pro správu, k němuž je zařízení připojeno, už není nastaven jako důvěryhodný

Stav	ⓘ
Součást	Ochrana připojení k serveru pro správu
ID události systému Windows	3303
ID události aplikace Kaspersky Security Center	00000ce7
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Asynchronous Sandbox detection

Stav	
Součást	Sandbox
ID události systému Windows	2619
ID události aplikace Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
Parametry události	• GNRL_EA_PARAM_1 jsou parametry součástí Sandbox. • GNRL_EA_PARAM_2 je cesta k příslušnému objektu. • GNRL_EA_PARAM_3 je ID incidentu. • GNRL_EA_PARAM_4 je hash objektu (SHA256).
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

The scan task has been successfully sent to Sandbox by a user

Stav	
Součást	Sandbox
ID události systému Windows	2622
ID události aplikace Kaspersky Security Center	00000a3e
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Device is connected

Stav	
Součást	Kontrola zařízení
ID události systému Windows	805
ID události aplikace Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Parametry události	• GNRL_EA_PARAM_1 je ID hardwaru (HWID). • GNRL_EA_PARAM_2 je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Device is disconnected

Stav	
Součást	Kontrola zařízení
ID události systému Windows	806
ID události aplikace Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED

Parametry události	• `GNRL_EA_PARAM_1` je ID hardwaru (HWID). • `GNRL_EA_PARAM_2` je jméno uživatele relace.
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Error removing the previous version of the application

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	`246`
ID události aplikace Kaspersky Security Center	`000000f6`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Successful connection to the EDR Expert server

Stav	ⓘ
Součást	Endpoint Detection and Response Expert (on-premise)
ID události systému Windows	`2853`
ID události aplikace Kaspersky Security Center	`00000b25`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Úspěšné připojení k serveru pro zpracování odpovědí EDR Expert

Stav	ⓘ
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	`2853`
ID události aplikace Kaspersky Security Center	`00000b25`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Úspěšné připojení k serveru pro shromažďování telemetrie EDR Expert

Stav	ⓘ
Součást	Endpoint Detection and Response Expert (on-premise) Endpoint Detection and Response Expert (cloud)
ID události systému Windows	`2857`
ID události aplikace Kaspersky Security Center	`00000b26`
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Úspěšné připojení k serveru NDR

Stav	ⓘ
Součást	Network Detection and Response (KATA)
ID události systému Windows	3083
ID události aplikace Kaspersky Security Center	00000c0b
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Starting the cloud service client application is allowed

Stav	ⓘ
Součást	Cloud Discovery
ID události systému Windows	2210
ID události aplikace Kaspersky Security Center	000008a2
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Access to the cloud service is allowed

Stav	ⓘ
Součást	Cloud Discovery
ID události systému Windows	2211
ID události aplikace Kaspersky Security Center	000008a3
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Přístup k chráněné oblasti

Stav	ⓘ
Součást	Audit systému
ID události systému Windows	2004
ID události aplikace Kaspersky Security Center	000007d4
Protokol událostí systému Windows (výchozí)	✓
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

File or folder change was detected

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2950
ID události aplikace Kaspersky Security Center	00000b86
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Object changes too often. Event aggregation started

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2955
ID události aplikace Kaspersky Security Center	00000b8b
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Report on object modification for the aggregation period

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2956
ID události aplikace Kaspersky Security Center	00000b8c
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Registry change was detected

Stav	/ /
Součást	Monitorování integrity systému
ID události systému Windows	2951
ID události aplikace Kaspersky Security Center	00000b87
Protokol událostí systému Windows (výchozí)	–

Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Device connection / disconnection is detected

Stav	ⓘ / ⚠ / ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2952
ID události aplikace Kaspersky Security Center	00000b88
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Součástí monitorování jsou nesprávné objekty

Stav	ⓘ / ⚠ / ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2903
ID události aplikace Kaspersky Security Center	00000b89
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Baseline created

Stav	ⓘ
Součást	Monitorování integrity systému
ID události systému Windows	2957
ID události aplikace Kaspersky Security Center	00000b8d
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Baseline updated

Stav	
Součást	Monitorování integrity systému
ID události systému Windows	2958
ID události aplikace Kaspersky Security Center	00000b8e
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

An operation is performed by the trusted user

Stav	
Součást	Monitorování integrity systému
ID události systému Windows	2962
ID události aplikace Kaspersky Security Center	00000b92
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Chcete-li nakonfigurovat dobu uchování pro tuto událost, přejděte do části zásad **Event configuration** a nastavte dobu uchování pro obecnou událost Sledování integrity systému – *File or folder change was detected*.

Connected to SVM

Stav	
Součást	Light Agent
ID události systému Windows	3152
ID události aplikace Kaspersky Security Center	00000c50
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

A new temporary password was created

Stav	
Součást	Audit systému
ID události systému Windows	265
ID události aplikace Kaspersky Security Center	00000109
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Connected to the Integration Server

Stav	ⓘ
Součást	Light Agent
ID události systému Windows	3105
ID události aplikace Kaspersky Security Center	00000c21
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Restoring connection to the Integration Server

Stav	ⓘ
Součást	Light Agent
ID události systému Windows	3104
ID události aplikace Kaspersky Security Center	00000c20
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Úspěšné připojení k serveru KUMA

Stav	ⓘ
Součást	Integrace KUMA
ID události systému Windows	2857
ID události aplikace Kaspersky Security Center	00000b29
Protokol událostí systému Windows (výchozí)	–
Protokol událostí aplikace Kaspersky Security Center (výchozí)	✓

Příloha 7. Podporované přípony souborů pro součást Prevence spouštění

Kaspersky Endpoint Security podporuje prevenci otevírání souborů ve formátu aplikací Office v určitých aplikacích. Informace o podporovaných příponách souborů a aplikací jsou uvedeny v následující tabulce.

Podporované přípony souborů pro součást Prevence spouštění

Název aplikace	Spustitelný soubor	Přípona souboru
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf

Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat	acrord32.exe	pdf
Foxit PDF Reader	FoxitReader.exe	
STDU Viewer	STDUViewerApp.exe	
Microsoft Edge	MicrosoftEdge.exe	
Google Chrome	chrome.exe	
Mozilla Firefox	firefox.exe	
Yandex Browser	browser.exe	
Tor Browser	tor.exe	

Příloha 8. Podporované překladače skriptů pro součást Prevence spouštění

Součást Prevence spouštění podporuje následující překladače skriptů:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe

- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Součást Prevence spouštění podporuje práci s aplikacemi v běhovém prostředí Java (procesy java.exe a javaw.exe).

Příloha 9. Rozsah kontroly IOC v registru (RegistryItem)

Když do rozsahu kontroly IOC přidáte datový typ **Windows registry - RegistryItem**, aplikace Kaspersky Endpoint Security kontroluje tyto klíče registru:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile
```

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Příloha 10. Požadavky na soubor IOC

Při vytváření úloh Kontrola IOC mějte na paměti tyto požadavky na soubory IOC a omezení:

- Aplikace podporuje soubory IOC s příponami IOC a XML v otevřeném standardu OpenIOC verze 1.0 a 1.1.
- Po nahrání souborů IOC můžete soubory ručně upravit v integrovaném editoru přímo ve vlastnostech úlohy. Kaspersky Endpoint Security podporuje úpravy souborů IOC, které jsou v souladu se standardem OpenIOC 1.1. Obsah souborů IOC kompatibilních s OpenIOC verze 1.0 není možné upravovat.
- Pokud při vytváření úlohy *IOC Scan* na příkazovém řádku nahrajete soubory IOC, z nichž některé nejsou podporovány, aplikace při provádění úlohy použije pouze ty podporované. Pokud se při vytváření úlohy *IOC Scan* na příkazovém řádku ukáže, že jsou všechny nahrávané soubory IOC nepodporované, úlohu lze i tak spustit, ale nezjistí žádné indikátory narušení. Nepodporované soubory IOC nelze nahrávat pomocí webové konzoly ani cloudové konzoly.
- Sémantické chyby a nepodporované výrazy a značky IOC v souborech IOC nezpůsobí chybu provádění úlohy. V těchto částech souborů IOC aplikace nezjistí žádnou shodu.
- Identifikátory všech souborů IOC používaných v jedné úloze Kontrola IOC musí být jedinečné. Pokud neexistují žádné soubory IOC se stejným identifikátorem, může to mít vliv na výsledky provádění úlohy.
- Velikost jednoho souboru IOC nesmí překročit 2 MB. Používání větších souborů povede k tomu, že úloha Kontrola IOC skončí chybou. Celková velikost všech souborů přidávaných do kolekce IOC by neměla být vyšší než 10 MB. Pokud celková velikost všech souborů přesáhne 10 MB, musíte kolekci IOC rozdělit a vytvořit několik úloh *IOC Scan*.
- Doporučujeme vytvářet jeden soubor IOC na hrozbu. Díky tomu je jednodušší analýza výsledků úlohy *IOC Scan*.

Soubor, který si můžete stáhnout kliknutím na níže uvedený odkaz, obsahuje tabulku s úplným seznamem podmínek IOC standardu OpenIOC.

STAŽENÍ SOUBORU IOC_TERMS.XLSX

Funkce a omezení podpory aplikace pro standard OpenIOC jsou uvedeny v následující tabulce.

Funkce a omezení podpory pro OpenIOC verze 1.0 a 1.1.

Podporované podmínky	OpenIOC 1.0:
	`is`
	`isnot` (jako výjimka za sady)
	`contains`
	`containsnot` (jako výjimka za sady)
	OpenIOC 1.1:
	`is`
	`contains`
	`starts-with`
	`ends-with`

	`matches`
	`greater-than`
	`less-than`
	U podmínek E-mail/* jsou podporovány pouze `contains` a `is`. Aby retrospektivní kontrola IOC fungovala správně, při použití podmínky `is` musí být e-mailové adresy v souborech IOC zadány v následujícím formátu: `"name@example.org" <SMTP:name@example.org>`. Při spuštění úlohy *Kontrola IOC* za normálních okolností postačí zadat e-mailovou adresu v následujícím formátu: `name@example.org`.

Podporované atributy podmínky	OpenIOC 1.1:
	`preserve-case`
	`negate`

Podporované operátory	`AND` `OR`
Podporované datové typy	`"date"`: datum (lze použít podmínky: `is`, `greater-than`, `less-than`) `"int"`: celé číslo (lze použít podmínky: `is`, `greater-than`, `less-than`) `"string"`: řetězec (lze použít podmínky: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: doba trvání v sekundách (lze použít podmínky: `is`, `greater-than`, `less-than`)

Funkce interpretace datového typu	Datové typy `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` a `"base64Binary"` jsou interpretovány jako řetězec.
	Aplikace podporuje interpretaci nastavení `Content` u datových typů `int` a `date`, pokud je nastaveno v podobě intervalů:
	OpenIOC 1.0:
	Používání operátoru `TO` v poli `Content`:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Používání podmínek `greater-than` a `less-than`
	Používání operátoru `TO` v poli `Content`
	Aplikace podporuje interpretaci datových typů `date` a `duration`, pokud jsou indikátory nastaveny ve formátu `ISO 8601, Zulu time zone, UTC`.

Příloha 11. Uživatelské účty v pravidlech součástí aplikace

Chcete-li nakonfigurovat některé součásti aplikace, musíte přidat speciální pravidla. Například pro součást Kontrola webu musíte přidat pravidlo se seznamem webových adres, které má aplikace blokovat. V pravidlech součásti aplikace můžete také nakonfigurovat plán pro danou součást nebo vybrat uživatele, na které má aplikace pravidlo aplikovat.

Pravidla je třeba přidat pro konfiguraci následujících součástí aplikace:

- Kontrola aplikací.
- Kontrola webu.
- Kontrola zařízení.
- Kontrola protokolu.
- Adaptivní kontrola anomálií.
- Monitorování integrity systému.

V pravidlech součástí aplikace Kaspersky Endpoint Security pro systém Windows můžete od verze 12.5 vybírat uživatele nejen z Active Directory, ale také ze seznamu uživatelů v aplikaci Kaspersky Security Center. Údaje o místním uživatelském účtu můžete zadat také ručně. To znamená, že můžete přidávat uživatele následujícími způsoby:

- Active Directory (doporučeno)
- Seznam uživatelů v aplikaci Kaspersky Security Center
- Místní uživatelský účet

Pro správné použití všech metod výběru uživatele je třeba aktualizovat aplikaci Kaspersky Endpoint Security a modul plug-in administrace na verzi 12.5 nebo vyšší.

Společnost Kaspersky doporučuje používat místní uživatelské účty pouze ve zvláštních případech, kdy není možné používat doménové uživatelské účty. Podrobnosti o bezpečnostních rizicích používání místních účtů naleznete ve znalostní bázi společnosti Microsoft. Při použití místních uživatelských účtů nesete plnou odpovědnost za bezpečnost počítače; to zahrnuje zejména odpovědnost za kontrolu a omezení přístupu k nastavení aplikace Kaspersky Endpoint Security.

Aplikace používá k identifikaci uživatelů SID (identifikátor zabezpečení) uživatele. Při používání uživatelských účtů ze služby Active Directory nebo ze seznamu uživatelů aplikace Kaspersky Security Center aplikace určí SID na serveru pro správu. To znamená, že aplikace pro identifikaci uživatele nezatěžuje počítač navíc. Pokud jste do pravidla aplikace přidali více než 1000 místních uživatelských účtů, aplikace kontaktují pro identifikaci uživatele řadič domény. To znamená, že se zvyšuje zatížení počítače. Chcete-li optimalizovat dopad na výkon počítače, doporučujeme používat uživatelské účty ze služby Active Directory nebo ze seznamu uživatelů aplikace Kaspersky Security Center.

Aplikace používá názvy pro NetBIOS pro identifikaci ručně přidaných uživatelských účtů ve formátech `<username>` a `<hostname>\<username>`. Název NetBIOS může být dlouhý až 16 bajtů (15 znaků). Pokud je název počítače delší než 15 znaků, aplikace nemůže uživatele identifikovat. Poté aplikace pravidlo zakáže a vygeneruje chybu, například *Web Control: rule triggering disabled for user accounts without matching security identifier (SID)*. Aby pravidlo fungovalo, musíte ručně zkrátit název počítače. Můžete přidat uživatelské účty ze služby Active Directory nebo aplikace Kaspersky Security Center. V takovém případě aplikace automaticky zkrátí název počítače.

Kaspersky Endpoint Security také podporuje v pravidlech integrované uživatele a skupiny (například skupinu „Vše“). Vzhledem k tomu, jak se určuje SID uživatele, aplikace umožňuje používat pouze integrované uživatelské účty přidané ze služby Active Directory nebo ze seznamu uživatelů v aplikaci Kaspersky Security Center. Pravidla, do nichž je místně přidán předdefinovaný uživatelský účet, nefungují.

Příloha 12. Rozhraní API pro reakci na hrozby EDR

Aplikace Kaspersky Endpoint Security 12.9 pro systém Windows zavádí podporu pro akce součásti Reakce na hrozby EDR (EDR responses) pomocí rozhraní OpenAPI aplikace Kaspersky Security Center. To znamená, že můžete volat metody OpenAPI za účelem automatizace reakce na hrozby EDR pomocí Pythonu. Tyto metody můžete volat po integraci s řešeními SIEM. *Kaspersky Unified Monitoring and Analysis Platform*, řešení Kaspersky SIEM, podporuje rozhraní OpenAPI součásti Reakce na hrozby EDR počínaje verzí 3.4.1. Ukázky skriptů najdete v dokumentaci KUMA.

Chcete-li provést akce součásti Reakce na hrozby EDR, musíte vytvořit žádost a odeslat ji pomocí rozhraní KSC Open API (`AddIncident`). Po zpracování žádosti je v konzole aplikace Kaspersky Security Center vytvořena zvláštní úloha.

Chcete-li vytvořit úlohy při reakci na hrozby EDR, musíte navázat připojení na pozadí mezi serverem pro správu a webovou konzolou aplikace Kaspersky Security Center. Služba připojení na pozadí je k dispozici v aplikaci Kaspersky Security Center pro systém Windows 14.2 nebo novější a v aplikaci Kaspersky Security Center Linux 15.2 a novější. Jiné konzoly, včetně konzol řešení Kaspersky Detection and Response, nejsou podporovány.

U součásti Reakce na hrozby EDR musíte zadat základní parametry požadavku, například ve formátu JSON:

- `task` je typ úlohy (viz níže).
- `targetHost` je ID počítače, na kterém musí být skript spuštěn. Povinný argument. Skript tento argument získá z události.
- `responseEventIncidentArea` je název aplikace, která spustila skript (například `KUMA`). Tento parametr se přidá do názvu vytvořené úlohy.

Chcete-li nakonfigurovat součást Reakce na hrozby EDR, musíte určit nastavení úlohy ve formátu JSON v parametru `"KLINCDT_BODY": json.dumps(data)`. V důsledku toho aplikace vytvoří úlohu `[Response][KUMA] <task type> - <Date> <Time> - <ID>` v konzole aplikace Kaspersky Security Center.

Připojování k rozhraní OpenAPI aplikace Kaspersky Security Center

V rámci součásti Reakce na hrozby EDR aplikace vytváří zvláštní úlohy v konzole aplikace Kaspersky Security Center. Vytvoření těchto úloh vyžaduje navázání připojení mezi počítačem a aplikací Kaspersky Security Center. Aby toho bylo dosaženo, musí být v žádosti zadány parametry připojení k aplikaci Kaspersky Security Center.

V Kaspersky XDR verze 2.1 se změnil způsob autorizace žádostí. Kaspersky XDR používá místo ověřování uživatelského jména a hesla tokeny PAT. V Kaspersky XDR proto nelze spouštět skripty. Další informace o autorizaci žádostí najdete v nápovědě k aplikaci Kaspersky XDR.

Parametry připojení k aplikaci Kaspersky Security Center

Parametr	Typ	Popis
`kscHost`	`string`	Adresa serveru pro správu Kaspersky Security Center. Povinný parametr.
`kscPort`	`int`	Port pro připojení k serveru pro správu. Povinný parametr.
`kscCert`	`string`	Cesta k souboru certifikátu pro připojení k serveru pro správu aplikace Kaspersky Security Center. Ve výchozím nastavení je parametr nastaven na `False`.
`kscUser`	`string`	Název uživatelského účtu Povinný parametr.
`kscPassword`	`string`	Heslo uživatelského účtu. Povinný parametr.

Příklad

```
# KSC connection info

# reads Environment variables by default, change with corresponding values

# KSC host, string, required

kscHost = "kscHost"

# KSC port, required, default is "13299"

kscPort = "13299"

# KSC certificate file path, default is False

kscCert = False

# KSC user, string, required

kscUser = "kscUser"

# KSC password, string, required

kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)

  server = KlAkAdmServer.Create(

    server_url, kscUser, kscPassword, verify=kscCert)

  params = validate(args)

  data = {"targetHost": <MyHost>,

      "task": task,

      "params": params,

      "responseEventIncident": True,

      "responseEventIncidentArea":"Kuma"}

  oHostGroup = KlAkHostGroup(server)

  incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,

                  "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),

                  "KLINCDT_BODY": json.dumps(data),

                  "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

  oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,

                   "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Data uživatelského účtu nejsou chráněna, proto musíte vyhradit samostatného uživatele, který bude sloužit pouze k provádění těchto akcí.

Načíst soubor – getFile

Nastavení úlohy Načíst soubor

Parametr	Typ	Popis
`md5hash`	`string`	Algoritmus MD5 hash souboru, který chcete načíst.
`sha256hash`	`string`	Algoritmus SHA256 hash souboru, který chcete načíst.
`path`	`string`	Cesta k souboru, který chcete načíst.

Příklad

```
type getFile = {
task: 'getFile';
targetHost: string;
params: {
// an empty string or a valid md5 hash of the file
md5hash: string;
// an empty string or a valid sha256 hash of the file
sha256hash: string;
// the path to the file
path: string;
};
responseEventIncidentArea: string;
};
```

Odstranit soubor – deleteFile

Nastavení úlohy Odstranit soubor

Parametr	Typ	Popis
`md5hash`	`string`	Algoritmus MD5 hash souboru, který chcete odstranit.
`sha256hash`	`string`	Algoritmus SHA256 hash souboru, který chcete odstranit.
`path`	`string`	Cesta k souboru, který chcete odstranit.
`searchInSubfolders?`	`boolean`	V podsložkách vyhledejte soubor, který chcete odstranit.

Příklad

```
type deleteFile = {
task: 'deleteFile';
targetHost: string;
params: {
// an empty string or a valid md5 hash of the file
md5hash: string;
// an empty string or a valid sha256 hash of the file
sha256hash: string;
// the path to the file
path: string;
// recursive search for a file (subfolder), optional
searchInSubfolders?: boolean;
};
responseEventIncidentArea: string;
};
```

Přesunout soubor do karantény – quarantineFile

Nastavení úlohy Přesunout soubor do karantény

Parametr	Typ	Popis
`md5hash`	`string`	Algoritmus MD5 hash souboru, který chcete umístit do karantény.
`sha256hash`	`string`	Algoritmus SHA256 hash souboru, který chcete umístit do karantény.
`path`	`string`	Cesta k souboru, který chcete umístit do karantény.

Příklad

```
type quarantineFile = {

task: 'quarantineFile';

targetHost: string;

params: {

// an empty string or a valid md5 hash of the file

md5hash: string;

// an empty string or a valid sha256 hash of the file

sha256hash: string;

// the path to the file

path: string;

};

responseEventIncidentArea: string;

};
```

Kontrola IOC – iocScan

Nastavení úlohy Kontrola IOC

Parametr	Typ	Popis
`ioc`	`string`	Cesta k archivu ZIP se souborem IOC, který chcete použít pro kontrolu.
`isolateHost`	`boolean`	Při zjištění indikátoru narušení izolujte počítač od sítě, abyste zabránili šíření hrozby.
`scanCriticalAreas`	`boolean`	Při zjištění indikátoru narušení spusťte úlohu *Kontrola kritických oblastí*.
`quarantineObject`	`boolean`	Při zjištění indikátoru narušení odstraňte škodlivý objekt. Před odstraněním objektu vytvoří aplikace Kaspersky Endpoint Security záložní kopii pro případ, že bude nutné objekt později obnovit. Kaspersky Endpoint Security přesune záložní kopii do karantény.

Příklad

```
type iocScan = {

task: 'iocScan';

targetHost: string;

params: {

// the path to the zip archive with ioc files in base64 encoding

ioc: string;

// isolation of the computer from the network

isolateHost: boolean;

// critical areas scan

scanCriticalAreas: boolean;

// quarantine the file

quarantineObject: boolean;

};

responseEventIncidentArea: string;

};
```

Spustit proces – startProcess

Nastavení úlohy Spustit proces

Parametr	Typ	Popis
`executablePath`	`string`	Cesta ke spustitelnému souboru, která se použije ke spuštění procesu.
`arguments?`	`string`	Další argumenty příkazového řádku pro spuštění procesu.
`workingFolder?`	`string`	Cesta k pracovní složce procesu.

Příklad

```
type startProcess = {
task: 'startProcess';
targetHost: string;
params: {
// the path to the file
executablePath: string;
// command line arguments, optional
arguments?: string;
// a working folder, optional
workingFolder?: string;
};
responseEventIncidentArea: string;
};
```

Ukončit proces – terminateProcess

Nastavení úlohy Ukončit proces

Parametr	Typ	Popis
`md5hash`	`string`	Algoritmus MD5 hash souboru, který chcete ukončit.
`sha256hash`	`string`	Algoritmus SHA256 hash souboru, který chcete ukončit.
`path`	`string`	Cesta k souboru, který chcete odstranit.
`caseSensitive`	`boolean`	Při hledání souboru se rozlišují malá a velká písmena.

Příklad

```
type terminateProcess = {
task: 'terminateProcess';
targetHost: string;
params: {
// an empty string or a valid md5 hash of the file
md5hash: string;
// an empty string or a valid sha256 hash of the file
sha256hash: string;
// the path to the file
path: string;
// case sensitive of the file name
caseSensitive: boolean;
};
responseEventIncidentArea: string;
};
```

Izolace počítače od sítě – isolateHost

Nastavení izolace počítače od sítě

Parametr	Typ	Popis
`action`	`string`	Provozní režim Izolace sítě.

Příklad

```
type isolateHost = {

task: 'isolateHost';

targetHost: string;

params: {

// 0 - turning off network isolation, 1 - turning on network isolation

action: number;

};

responseEventIncidentArea: string;

};
```

Prevence spouštění – preventExecution

Nastavení prevence spouštění

Parametr	Typ	Popis
`hash`	`string`	Algoritmus MD5 hash souboru, jehož spuštění chcete zabránit.
`path`	`string`	Cesta k souboru, jehož spuštění chcete zabránit.
`caseSensitive`	`boolean`	Při hledání souboru se rozlišují malá a velká písmena.

Příklad

```
type preventExecution = {

task: 'preventExecution';

targetHost: string;

params: {

// a valid md5 hash of the file

hash: string;

// the path to the file

path: string;

// case sensitive of the file name

caseSensitive: boolean;

};

responseEventIncidentArea: string;

};
```

Kontrola malwaru – onDemandScan

Nastavení úlohy Kontrola malwaru

Parametr	Typ	Popis
`path`	`string`	Seznam souborů a složek pro vlastní kontrolu oddělených mezerami.
`recursive`	`boolean`	Režim rekurzivní kontroly.
`type`	`number`	Rozsah kontroly.

```
ScanObjectType = Enum("ScanObjectType",
```

[

("SystemMemory", 14),

("StartupObjectsAndRunningProcesses", 15),

("DiskBootSectors", 16),

("SystemBackupStorage", 17),

("Email", 18),

("Folder", 22),

("AllRemovableDrives", 23),

("AllNetworkDrives", 24),

("AllFixedDrives", 25)])

Příklad

```
type onDemandScan = {

task: 'onDemandScan';

targetHost: string;

// please note, this is an array

// array of scan object

params: [{

// enabling the scan object

enabled: boolean;

// an empty string or the path to the folder to scan

path: string;

// recursive scan mode

recursive: boolean;

// ID scan object

type: number;

}];

responseEventIncidentArea: string;

};
```

Informace o kódu třetích stran

Informace o kódu třetích stran je obsažená v souboru legal_notices.txt 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 v USA a/nebo dalších zemích.

Amazon, Amazon Web Services, AWS jsou ochranné známky společnosti Amazon.com, Inc. nebo jejích přidružených společností.

Apple, FireWire, iTunes, Mac a Safari jsou ochranné známky společnosti Apple Inc.

Arm je registrovaná ochranná známka společnosti Arm Limited (nebo dceřiných společností) v USA a/nebo jiných 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.

Cisco, Cisco AnyConnect, IOS jsou registrované ochranné známky společnosti Cisco Systems, Inc. a/nebo jejích dceřiných společností v USA a určitých dalších zemích.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop a XenServer jsou registrované ochranné známky nebo ochranné známky společnosti Cloud Software Group, Inc. a/nebo jejích poboček v USA a/nebo jiných zemích.

Cloudflare, Cloudflare Workers a logo Cloudflare jsou ochranné známky a/nebo registrované ochranné známky společnosti Cloudflare, Inc. v USA a dalších jurisdikcích.

Core je ochranná známka společnosti Intel Corporation nebo jejích dceřiných společností.

dBase je ochranná známka společnosti dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC a další ochranné známky jsou ochranné známky společnosti Dell Inc. nebo jejích dceřiných společností.

Docker a logo Docker jsou ochranné známky nebo registrované ochranné známky společnosti Docker, Inc. v USA a/nebo dalších zemích. Společnost Docker, Inc. a další strany mohou mít práva na ochranné známky i k jiným výrazům používaných v tomto dokumentu.

ESET je ochranná známka nebo registrovaná ochranná známka společnosti ESET spol. s r.o. nebo příslušného subjekt ESET.

Foxit je registrovaná ochranná známka společnosti Foxit Corporation.

Radmin je registrovaná ochranná známka společnosti Famatech.

Google, Android, Google Public DNS, Google Chrome a Chrome jsou ochranné známky společnosti Google LLC.

HUAWEI, FusionCompute a FusionSphere jsou ochranné známky společnosti Huawei Technologies Co., Ltd.

ICQ je ochranná známka a/nebo značka služby společnosti ICQ LLC.

Intel je ochranná známka společnosti Intel Corporation nebo jejích dceřiných společností.

IBM je ochranná známky společnosti International Business Machines Corporation zaregistrovaná v mnoha jurisdikcích po celém světě.

Lenovo a Lenovo 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 LLC nebo jejích dceřiných společností v USA a/nebo dalších zemích.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server a Windows Store jsou registrované ochranné známky skupiny společností Microsoft.

Mozilla, Firefox a Thunderbird jsou ochranné známky společnosti Mozilla Foundation v USA a dalších zemích.

NetApp je ochranná známka nebo registrovaná ochranná známka společnosti NetApp, Inc. v USA a/nebo dalších zemích.

OpenSSL je ochranná známka vlastněná společností OpenSSL Software Foundation.

OpenStack je registrovaná ochranná známka společnosti OpenStack Foundation v USA a dalších zemích.

Oracle, Java a JavaScript jsou registrované ochranné známky společnosti Oracle a/nebo jejích dceřiných společností.

Python je ochranná známka nebo registrovaná ochranná známka společnosti Python Software Foundation.

Realtek je ochranná známka společnosti Realtek Semiconductor Corporation.

SAMSUNG je ochranná známka společnosti SAMSUNG v USA nebo dalších zemích.

Thawte je ochranná známka nebo registrovaná ochranná známka společnosti Symantec Corporation nebo jejích dceřiných společností v USA a dalších zemích.

Trend Micro je ochranná známka nebo registrovaná ochranná známka společnosti Trend Micro Incorporated.

VERISIGN je registrovaná ochranná známka v USA a dalších zemích nebo neregistrovaná ochranná známka společnosti VeriSign, Inc. a jejích dceřiných společností.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere jsou registrované ochranné známky a/nebo ochranné známky společnosti VMware, Inc. V USA a dalších zemích.