ESET Endpoint Security

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

ESET Endpoint Security byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte https://www.eset.cz.

Technická podpora: https://servis.eset.cz

REV. 2024-04-12

ESET Endpoint Security

ESET Endpoint Security představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ESET LiveGrid® v kombinaci s vlastním Firewallem a Antispamovou ochranou poštovních klientů využívá rychlost a přesnost k zajištění bezpečnosti vašeho zařízení. Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET Endpoint Security je komplexní bezpečnostní řešení, které nabízí výkonnou a účinnou ochranu při zachování minimálního dopadu na výkon systému. Pokročilé technologie založené na umělé inteligenci jsou schopny proaktivně eliminovat viry, spyware, trojské koně, červy, adware, rootkity a další internetové hrozby, bez znatelného dopadu na výkon počítače nebo funkčnost operačního systému.

ESET Endpoint Security je primárně navržen pro ochranu pracovních stanic v SMB prostředí.

V kapitole Instalace naleznete témata nápovědy rozdělená do několika podkapitol, které vám poskytnou orientaci a kontext, včetně informací o stažení, instalaci a aktivaci.

Pomocí nástroje ESET PROTECT můžete v enterprise prostředí snadno spravovat libovolné množství klientských stanic – aplikovat na ně politiky, sledovat detekce a vzdáleně ESET Endpoint Security konfigurovat z jakéhokoli počítače v síti.

Nejčastěji kladené dotazy a řešené problémy naleznete v kapitole Časté otázky.

Funkce a přednosti

Přepracované uživatelské rozhraní	Uživatelské rozhraní produktu bylo kompletně přepracováno. Nyní je čistější, přehlednější a intuitivnější. Upravili jsme textaci oznámení zobrazených uživateli a přidali také podporu pro jazyky se zápisem zprava doleva, jako je Hebrejština a Arabština. Prostřednictvím online nápovědy, integrované do produktu, získáte vždy nejaktuálnější informace ke konkrétním zobrazeným oknům v programu ESET Endpoint Security.
Tmavý režim	Rozšíření pro zapnutí tmavého zobrazení uživatelského rozhraní. Preferované barevné schéma si můžete zvolit v prvcích uživatelského rozhraní.
Antivirus a antispyware	Proaktivně detekuje a léčí známé i neznámé viry, červy, trojské koně a rootkity. Pokročilá heuristika označí každý dosud neznámý škodlivý kód, chrání vás před neznámými hrozbami a eliminuje je dříve, než mohou způsobit škodu. Ochrana přístupu na web a modul Anti-Phishing monitoruje komunikaci mezi internetovým prohlížečem a vzdálenými servery (včetně SSL). Ochrana poštovních klientů zajišťuje kontrolu komunikace pomocí POP3(S) a IMAP(S) protokolů.
Pravidelné aktualizace	Pravidelné aktualizace detekční jádra (dříve známé jako "virové databáze") a programových modulů zajistí maximální ochranu počítače.
ESET LiveGrid® (založen na cloudové technologii)	Můžete zkontrolovat reputaci spuštěných procesů a souborů přímo v ESET Endpoint Security vůči cloudové databázi.
Vzdálená správa	ESET PROTECT je aplikace, prostřednictvím které můžete spravovat bezpečnostní produkty ESET na stanicích, serverech i mobilních zařízeních z jednoho centrálního místa v síti. Prostřednictvím ESET PROTECT Web Console (ESET PROTECT Web Console) můžete vzdáleně instalovat bezpečnostní řešení ESET na zařízení, spravovat jejich konfiguraci a rychle reagovat na nové problémy a hrozby v síti.

Ochrana proti síťovým útokům	Tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Komunikace, která bude vyhodnocena jako škodlivá, bude blokována.
Filtrování obsahu webu (pouze v ESET Endpoint Security)	Filtrování obsahu webu umožňuje blokovat webové stránky s potenciálně urážlivým obsahem. Kromě toho můžete jako zaměstnavatel/administrátor zakázat přístup na 27 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

Co je nového?

Co je nového v ESET Endpoint Security verze 10.1

Zabezpečení všech prohlížečů

Všechny podporované webové prohlížeče se automaticky spustí v zabezpečeném režimu. Díky tomu můžete prohlížet webové stránky, používat internetové bankovnictví a provádět online transakce v jednom zabezpečeném prohlížeči bez vynuceného přesměrování konkrétních stránek.

Nový editor pravidel firewallu

Editor pravidel firewallu byl přepracován tak, aby umožňoval snadnější definování pravidel firewallu s většími možnostmi konfigurace.

Intel® Threat Detection Technology

Hardwarová technologie odhalující ransomware, který se pokouší vyhnout detekci v paměti. Její integrace zvyšuje ochranu proti ransomware a nemá negativní vliv na výkon systému. Viz podporované procesory.

Tmavý režim a přepracované uživatelské rozhraní

Grafické uživatelské rozhraní (GUI) bylo v této verzi bylo přepracováno a modernizováno. Tato funkce umožňuje kromě světlého barevného schématu uživatelského rozhraní ESET Endpoint Security zvolit schéma tmavé, případně barevné schéma dle systému, viz kapitola Prvky uživatelského rozhraní.

Přepracovaná Rozšířená nastavení

Rozšířená nastavení byla přepracována a jednotlivá nastavení jsou nyní seskupena s ohledem na větší pohodlí uživatele.

Opravena řada chyb a další výkonová vylepšení.

Systémové požadavky

Pro plynulý běh produktu ESET Endpoint Security (ve výchozím nastavení) by váš systém měl splňovat následující hardwarové a softwarové požadavky:

Podporované procesory

Intel nebo AMD procesor, 32-bit (x86) s instrukční sadou SSE2 nebo 64-bit (x64), 1 GHz a rychlejší

ARM64 procesor, 1 GHz a rychlejší

Operační systémy

Microsoft® Windows® 11

Microsoft® Windows® 10

Podrobný seznam podporovaných verzí Microsoft® Windows® 10 a Microsoft® Windows® 11 naleznete v samostatném článku s přehledem podpory operačního systému Windows.

Vždy se snažte udržovat svůj operační systém aktualizovaný.

Pro instalaci nebo aktualizaci produktů ESET vydaných po červenci 2023 musí být ve všech operačních systémech Windows nainstalována podpora pro Azure Code Signing. Přečtete si článek o používání produktu ESET na zařízeních s Windows 7 and Windows 8.1.

Požadavky funkcí produktu ESET Endpoint Security

V tabulce níže naleznete přehled systémových požadavků konkrétních funkcí produktu ESET Endpoint Security:

Funkce	Požadavky
Intel® Threat Detection Technology	Viz podporované procesory.
Zabezpečený prohlížeč	Viz podporované prohlížeče.
ESET Specialized Cleaner	Procesor nezaložený na architektuře ARM64.
Exploit Blocker	Procesor nezaložený na architektuře ARM64.
Hloubková analýza chování	Procesor nezaložený na architektuře ARM64.
Zabezpečený prohlížeč – přesměrování webových stránek	Procesor nezaložený na architektuře ARM64.

Instalační balíček ESET Endpoint Security vytvořený pomocí ESET PROTECT podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 v režimu více relací.

Ostatní

- Hardware musí splňovat systémové požadavky pro běh samotného operačního systému a dalších aplikací na něm provozovaných
- 300 MB volné operační paměti (viz poznámku 1)
- 1 GB volného místa na disku (viz poznámku 2)
- Minimální rozlišení obrazovky 1024 x 768
- Připojení k internetu nebo do lokální sítě, ve které se nachází server poskytující aktualizace produktu (viz poznámka 3)
- Souběžné používání dvou antivirových programů na jednom systému povede nevyhnutelně ke konfliktu v přístupu k systémovým prostředkům, což se projeví jeho zpomalením a může vést k jeho nefunkčnosti

Na počítač, který nesplňuje minimální požadavky, se zpravidla produkt ESET podaří nainstalovat, ale toto doporučujeme pouze pro testovací provoz, a zjištění výkonových nároků.

(1) V některých případech může produkt spotřebovat více operační paměti, pokud je dostupná. Například pokud se na počítači nachází velké množství hrozeb nebo při importování velkého množství dat (například seznamů povolených stránek).

(2) Místo na disku je potřeba pro stažení instalačního balíčku, samotnou aktualizaci produktu a následné zazálohování instalačního balíčku do programové složky. Program na disk ukládá zálohy aktualizovaných modulů, aby bylo možné se v případě potíží vrátit ke starší verzi. V závislosti na nastavení produktu se na disk může ukládat velké množství protokolů a výpisy paměti. Karanténa, do které se ukládají nalezené hrozby, které dosud neexistovaly, se rovněž ukládají na pevný disk. Pro plynulou aktualizaci bezpečnostního produktu ESET i operačního systému doporučujeme mít na disku vždy dostatek volného místa.

(3): V případě potřeby je možné produkt aktualizovat ručně z výměnného média, ale není to doporučováno.

Podporované jazyky

ESET Endpoint Security si můžete stáhnout a nainstalovat v níže uvedených jazycích.

Jazyk	Kód jazyka	LCID
Angličtina (Spojené státy americké)	en-US	1033
Arabština (Egypt)	ar-EG	3073
Bulharština	bg-BG	1026
Zjednodušená čínština	zh-CN	2052
Tradiční čínština	zh-TW	1028
Chorvatština	hr-HR	1050
Čeština	cs-CZ	1029
Estonština	et-EE	1061
Finština	fi-FI	1035
Francouzština (Francie)	fr-FR	1036
Francouzština (Kanada)	fr-CA	3084
Němčina (Německo)	de-DE	1031
Řečtina	el-GR	1032
*Hebrejština	he-IL	1037
Maďarština	hu-HU	1038
*Indonéština	id-ID	1057
Italština	it-IT	1040
Japonština	ja-JP	1041
Kazachština	kk-KZ	1087
Korejština	ko-KR	1042
*Lotyština	lv-LV	1062
Litevština	lt-LT	1063
Nederlands	nl-NL	1043
Norština	nb-NO	1044
Polština	pl-PL	1045
Portugalština (Brazílie)	pt-BR	1046
Rumunština	ro-RO	1048

Jazyk	Kód jazyka	LCID
Ruština	ru-RU	1049
Španělština (Chile)	es-CL	13322
Španělština (Španělsko)	es-ES	3082
Švédština (Švédsko)	sv-SE	1053
Slovenština	sk-SK	1051
Slovinština	sl-SI	1060
Thajština	th-TH	1054
Turečtina	tr-TR	1055
Ukrajinština (Ukrajina)	uk-UA	1058
*Vietnamština	vi-VN	1066

* V tomto jazyce je dostupný pouze ESET Endpoint Security, nikoli online uživatelská příručka (přesměrováni budete na anglickou verzi).

Chcete-li změnit jazyk této online uživatelské příručky, podívejte se do pole pro výběr jazyka (v pravém horním rohu).

Seznam změn

Prevence

Při používání počítače, zejména při práci s internetem, je potřeba mít neustále na paměti, že žádný antivirový systém nedokáže zcela odstranit riziko detekcí a vzdálených útoků. Pro zajištění maximální bezpečnosti a pohodlí je potřeba antivirové řešení správně používat a dodržovat několik užitečných pravidel:

Pravidelná aktualizace antivirového systému

Podle statistik z ESET LiveGrid® vznikají denně tisíce nových unikátních infiltrací, které se snaží obejít zabezpečení počítačů a přinést svým tvůrcům zisk. Viroví analytici společnosti ESET tyto hrozby denně analyzují a vydávají aktualizace, které zvyšují úroveň ochrany uživatelů antivirového systému. Při nesprávném nastavení aktualizace se účinnost antivirového systému dramaticky snižuje. Podrobnější informace, jak správně nastavit aktualizace produktu, naleznete v kapitole Nastavení aktualizace.

Stáhněte si aktualizace co nejdříve poté, co byly vydány.

Autoři škodlivého softwaru často využívají různé slabiny systému, aby zvýšili efektivitu šíření škodlivého kódu. Výrobci většiny programů proto pravidelně vydávají bezpečnostní záplaty, které chyby v produktech opravují a snižují tak riziko potenciální nákazy. Důležité je stáhnout tyto aktualizaci co nejdříve poté, co byly vydány. Mezi takové programy, které jsou aktualizovány pravidelně, můžeme zařadit například operační systém Windows nebo internetový prohlížeč Internet Explorer.

Zálohování důležitých dat

Tvůrci škodlivého kódu většinou neberou ohled na potřeby uživatelů. Infiltrace tak mohou způsobit částečnou nebo úplnou nefunkčnost programů, operačního systému nebo poškození dat, někdy dokonce i záměrně. Pravidelné zálohování důležitých a citlivých dat na externí zdroj, jako je DVD nebo externí pevný disk je více než nutné. Výrazně tím usnadníte a urychlíte případnou obnovu dat po pádu systému.

Pravidelná kontrola počítače

Detekci známých i neznámých virů, červů, trojských koní a rootkitů zajišťuje rezidentní ochrana souborového systému. Při každém přístupu k souboru tak dochází k jeho kontrole. Přesto vám doporučujeme, abyste prováděli ruční kontrolu počítače alespoň jednou měsíčně, protože signatury malwaru se mohou lišit. Aktualizace detekčního jádra probíhá denně.

Dodržování základních bezpečnostních pravidel

Nejužitečnější a nejúčinnější pravidlo ze všech – vždy buďte opatrní. V dnešní době je provedení a distribuce mnoha infiltrací závislé na prvním zásahu ze strany uživatele. Pokud budete při otevírání nových souborů opatrní, ušetříte si čas, který byste jinak trávili léčením počítače od škodlivého kódu. Několik užitečných rad:

- Omezte návštěvy podezřelých stránek, které uživatele bombardují otevíráním oken s reklamními nabídkami apod.
- Dbejte zvýšené opatrnosti při stahování a instalaci volně šiřitelných programů, kodeků apod. Doporučujeme používat pouze ověřené programy a navštěvovat bezpečné internetové stránky.
- Dbejte zvýšené opatrnosti při otevírání příloh e-mailů zvláště u hromadně posílaných zpráv nebo u zpráv od neznámých odesílatelů.
- Nepoužívejte pro běžnou práci na počítači účet s oprávněním Administrátora.

Nápověda programu

Vítejte v uživatelském manuálu ESET Endpoint Security. Věříme, že informace obsažené v této nápovědě vás seznámí s produktem a pomohou vám zabezpečit počítač.

Jak začít

Nezapomeňte, že ESET Endpoint Security můžete spravovat vzdáleně pomocí ESET PROTECT. Doporučujeme vám také seznámit se s počítačovými infiltracemi a útoky, se kterými se můžete setkat při používání svého počítače.

O nových funkcích v ESET Endpoint Security si můžete přečíst zde. Připravili jsme také průvodce, který vám pomůže se základním nastavením ESET Endpoint Security.

Jak používat nápovědu programu ESET Endpoint Security

Stránky nápovědy jsou pro lepší orientaci logicky uspořádány do jednotlivých kapitol a podkapitol. Související informace tak naleznete jednoduchým procházením této struktury stránek.

V případě, že potřebujete získat více informací pro konkrétní okno uživatelského rozhraní, stiskněte klávesu **F1**. Následně se otevře nápověda programu s obsahem pro dané okno.

Nápověda umožňuje vyhledávání prostřednictvím klíčových slov (záložka "Rejstřík" v levé části okna nápovědy) nebo pomocí vyhledání slov a slovních spojení (záložka "Hledat"). Rozdíl mezi těmito dvěma typy vyhledávání je ten, že klíčová slova se váží ke stránkám nápovědy logicky, přičemž samotné klíčové slovo se vůbec v textu nemusí vyskytovat. Vyhledávání pomocí slov a slovních spojení naopak najde všechny stránky nápovědy, na kterých se hledaná slova nachází přímo v textu.

Z důvodu zachování konzistence a zabránění nejasnostem vychází použitá terminologie v této příručce z názvosloví ESET Endpoint Security. Používáme rovněž jednotnou sadu symbolů na zvýraznění částí kapitol, které jsou zvlášť důležité, případně by neměly uniknout vaší pozornosti.

Poznámka je krátký výtah informace. Ačkoli ji můžete vynechat, poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.

Tato část vyžaduje vaši pozornost a doporučujeme ji nevynechat. Obvykle obsahuje nekritické, avšak důležité informace.

Takto označená informace vyžaduje vaši plnou pozornost. Varování jsou umístěna tak, aby vás včas varovala a zároveň vám pomohla vyvarovat se chybám, které by mohly mít negativní následky. Prosím, důkladně si přečtěte text ohraničený tímto označením, protože se týká velmi citlivých systémových nastavení nebo upozorňuje na možná rizika.

Příklad popisující uživatelský scénář nebo praktickou ukázku pro pochopení fungování nebo používání dané funkce.

Konvence	Význam
Tučné písmo	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.
Kurzíva	Zástupné znaky pro informace, které máte zadat. Například název souboru nebo cesta k souboru znamená, že máte zadat skutečnou cestu nebo název souboru.
`Courier New`	Příklady kódů nebo příkazů
Hypertextový odkaz	Poskytuje rychlý přístup do odkazovaných kapitol nebo externích zdrojů. Hypertextové odkazy jsou zvýrazněny modře a mohou být podtržené.
%ProgramFiles%	Systémová složka operačního systému Windows, do které se standardně instalují programy a další součásti systému.

Online příručka je primárním zdrojem nápovědy. V případě funkčního připojení k internetu se automaticky zobrazí nejnovější verze online příručky.

Příručka pro vzdáleně spravované produkty

ESET Endpoint Security a další produkty ESET určené pro ochranu firemních zařízení (stanic, serverů i mobilních zařízeních) je možné spravovat z jednoho centrálního místa v síti. Administrátoři, kteří spravují více než 10 klientských stanic by měli zvážit instalaci ESET nástroje pro vzdálenou správu, prostřednictvím kterého mohou nasazovat ESET produkty, spouštět úlohy, vynutit bezpečnostní politiky, monitorovat stav produktu a rychle reagovat na nově vniklé problémy nebo hrozby.

ESET nástroje pro vzdálenou správu

ESET Endpoint Security můžete vzdáleně spravovat prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud.

- Představení ESET PROTECT
- Představení ESET PROTECT Cloud

- ESET HUB – centrální brána k jednotné bezpečnostní platformě ESET PROTECT. Poskytuje centralizovanou správu identit, předplatného a uživatelů pro všechny moduly platformy ESET. Návod k aktivaci ESET PROTECT naleznete v kapitole Správa licencí. ESET HUB zcela nahradí ESET Business Account a ESET MSP Administrator.

- ESET Business Account – portál pro správu licencí pro firemní produkty ESET. Návod k aktivaci ESET PROTECT naleznete v kapitole Správa licencí nebo v online nápovědě k ESET Business Account, kde najdete další informace o používání ESET Business Account. Pokud máte k dispozici pouze uživatelské jméno a heslo, na tomto portále si je můžete převést na licenční klíč.

Další bezpečnostní produkty

- ESET Inspect – je komplexní Endpoint Detection and Response (EDR) systém, který nabízí následující funkce: detekce incidentů, správu incidentu a reakce na ně, sběr dat, indikaci na kompromitaci systémů, detekci anomálií, detekci chování a poručení firemní politiky.
- ESET Endpoint Encryption – je komplexní bezpečnostní aplikace navržená tak, aby chránila vaše uložená i přenášená data. Pomocí ESET Endpoint Encryption můžete šifrovat soubory, složky a e-maily nebo vytvářet šifrované virtuální disky, komprimovat archivy a bezpečné odstraňovat soubory.

Nástroje třetích stran pro vzdálenou správu

- Vzdálené monitorování a správa (RMM)

Osvědčené postupy

- Připojte všechny stanice s nainstalovaným ESET Endpoint Security do ESET PROTECT
- Ochraňte na spravovaných stanicích heslem přístup do rozšířeného nastavení a zabraňte neautorizovaným změnám v konfiguraci produktu
- Aplikujte na stanice politiky s doporučeným nastavením
- Změňte režim uživatelského rozhraní a omezte množství zobrazovaných informací produktem ESET Endpoint Security uživateli

Jak na to

- Jak dočasně změnit nastavení vynucené politikou?
- Jak nasadit ESET Endpoint Security prostřednictvím GPO nebo SCCM

Představení ESET PROTECT

ESET PROTECT je aplikace, prostřednictvím které můžete spravovat bezpečnostní produkty ESET na stanicích, serverech i mobilních zařízeních z jednoho centrálního místa v síti.

Prostřednictvím ESET PROTECT Web Console můžete vzdáleně nasazovat ESET produkty, spouštět úlohy, vynutit bezpečnostní politiky, monitorovat stav produktu a rychle reagovat na nově vniklé problémy nebo hrozby. Viz Přehled architektury a prvků infrastrukturyESET PROTECT, Začínáme s webovou konzolí ESET PROTECT a Podporovaná Desktop Provisioning prostředí.

ESET PROTECT se skládá z následujících komponent:

- ESET PROTECT Server – zajišťuje komunikaci mezi klientskými stanicemi (agenty) a uchovává data v

databázi. ESET PROTECT Server můžete nainstalovat na Windows, Linux nebo jej do virtuální prostředí nasadit jako virtuální appliance.

- ESET PROTECT Web Console – jedná se o primární rozhraní pro správu počítačů ve vaší síti. Zobrazuje přehled stavu klientů v síti a umožňuje vzdáleně nasadit řešení ESET na nespravované počítače. Jedná se o webové rozhraní, k jehož používání vám postačí webový prohlížeč. Pokud máte webový server dostupný z internetu, můžete ESET PROTECT spravovat prakticky odkudkoli z libovolného zařízení s internetovým prohlížečem.
- ESET Management Agent – komponenta, která zajišťuje komunikaci mezi klientskou stanicí a ESET PROTECT Serverem. Agenta je třeba nainstalovat na každé klientské zařízení pro navázání komunikace mezi ním a ESET PROTECT Serverem. Instalaci můžete provést lokálně nebo vzdáleně. Díky tomu, že je agent přímo na klientském počítači a může ukládat více bezpečnostních scénářů, výrazně se zkracuje reakční doba ESET Management Agenta na nové detekce. Agenta můžete prostřednictvím ESET PROTECT Web Console nasadit na nespravované stanice, jejichž seznam jste získali synchronizací s Active Directory, případně je detekoval ESET RD Sensor. Pokud je to nutné, můžete si na klientské počítače nainstalovat ESET Management Agenta také ručně.
- ESET Rogue Detection Sensor – nástroj, který vyhledává nespravovaná zařízení v síti a zasílá informace o nich na ESET PROTECT Server. Představuje tak pohodlný způsob pro přidání nových počítačů do ESET PROTECT bez nutnosti jejich ručního vyhledávání a zadávání. Rogue Detection Sensor si pamatuje počítače, které již objevil, a neodesílá duplicitní informace.
- ESET Bridge – je služba, kterou v kombinaci s ESET PROTECT můžete použít:
    - Jako cache, ze které se budou klientům distribuovat aktualizace detekčních modulů a ESET Management Agentovi instalační balíčky.
    - Pro přesměrování komunikace ESET Management Agentů na ESET PROTECT Server.
- Mobile Device Connector – komponenta pro Správu mobilních zařízení s ESET PROTECT. Zajišťuje komunikaci s mobilními zařízeními s OS Android (a aplikací ESET Endpoint Security pro Android), případně operačním systémem iOS.
- ESET PROTECT Virtuální appliance – připravený virtuální stroj s ESET PROTECT určený pro provoz ve virtuálním prostředí.
- ESET PROTECT Virtual Agent Host – komponenta ESET PROTECT, která virtualizuje entity agentů ke správě virtuálních strojů bez agentů. Toto řešení vám přináší do agent-less prostředí stejné možnosti automatizace, využití dynamických skupin a správy úloh jako v případě fyzických stanic, na kterých je nainstalován ESET Management Agent. Virtual Agent sbírá informace z virtuálních strojů a zasílá je na ESET PROTECT Server.
- Mirror Tool – představuje řešení pro aktualizace modulů v sítích bez přístupu k internetu. Prostřednictvím tohoto nástroje vytvoříte lokální kopii aktualizačních serverů i online repozitáře s instalačními balíčky.
- Remote Deployment Tool – prostřednictvím tohoto nástroje můžete vzdáleně nasadit all-in-one instalační balíček vytvořený v <%PRODUCT%> Web Console. Jedná se o pohodlný způsob, jak na stanice můžete vzdáleně nasadit ESET Management Agenta společně s bezpečnostním produktem ESET.

Více informací o dočasné změně nastavení naleznete v online dokumentaci ESET PROTECT.

Představení ESET PROTECT Cloud

Prostřednictvím ESET PROTECT Cloud můžete spravovat bezpečnostní produkty ESET na stanicích a serverech z jednoho centrálního místa, kdy k jeho provozu nepotřebujete fyzický ani virtuální server jako v případě ESET PROTECT. Přímo z ESET PROTECT Cloud Web Console můžete vzdáleně instalovat bezpečnostní řešení ESET na zařízení, spravovat jejich konfiguraci a rychle reagovat na nové problémy a hrozby na spravovaných počítačích.

ESET PROTECT Cloud se skládá z následujících komponent:

- Instance ESET PROTECT Cloud – zajišťuje komunikaci mezi klientskými stanicemi (agenty) a uchovává data v databázi.
- ESET PROTECT Cloud Web Console – jedná se o primární rozhraní pro správu počítačů ve vaší síti. Poskytuje přehled o všech klientech v síti a umožňuje vzdáleně nasadit agenta a bezpečnostní řešení ESET na počítače, které zatím prostřednictvím Web Console nespravujete. ESET PROTECT Cloud můžete používat z libovolného místa nebo zařízení s připojením k internetu.
- ESET Management Agent – komponenta, která zajišťuje komunikaci mezi klientskou stanicí a ESET PROTECT Cloud. Agent musí být nainstalován v klientském zařízení, aby bylo možné navázat komunikaci mezi tímto zařízením a serverem ESET PROTECT Cloud. Díky tomu, že je agent přímo na klientském počítači a může ukládat více bezpečnostních scénářů, výrazně se zkracuje reakční doba ESET Management Agenta na nové detekce. Pomocí webové konzoleESET PROTECT Cloud můžete nasadit ESET Management Agenta do zatím nespravovaných zařízení. Pokud je to nutné, můžete si na klientské počítače nainstalovat ESET Management Agenta také ručně.
- ESET Bridge – je služba, kterou v kombinaci s ESET PROTECT Cloud můžete použít:
    - Jako cache, ze které se budou klientům distribuovat aktualizace detekčních modulů a ESET Management Agentovi instalační balíčky.
    - Pro přesměrování komunikace ESET Management Agentů na ESET PROTECT Cloud.
- Správa mobilních zařízení – je komponenta pro správu mobilních zařízení pomocí ESET PROTECT Cloud, která umožňuje spravovat mobilní zařízení (Android a iOS) a spravovat ESET Endpoint Security for Android.
- Správa zranitelností a záplat – funkce ESET PROTECT Cloud, která pravidelně kontroluje pracovní stanici a detekuje nainstalovaný software, který by mohl být vystaven bezpečnostním rizikům. Správa záplat pomáhá tyto problémy řešit pomocí automatických aktualizací softwaru a udržuje tak zařízení ve větším bezpečí.

Více informací o dočasné změně nastavení naleznete v online dokumentaci ESET PROTECT Cloud.

Ochrana produktu heslem

Pro zajištění maximálního zabezpečení systému je nutné zajistit správnou konfiguraci ESET Endpoint Security. Jakákoli neoprávněná změna v jeho nastavení může vést ke snížení zabezpečení a úrovně ochrany. Abyste zamezili uživatelům v přístupu do rozšířeného nastavení a provádění změn, můžete nastavení produktu ochránit heslem.

Administrátor může vytvořit politiku, a na spravovaných počítačích hromadně nastavit heslo pro ochranu rozšířeného nastavení produktu ESET Endpoint Security. Pro vytvoření nové politiky:

1. V hlavním menu ESET PROTECT Web Console klikněte na **Politiky**.
2. Klikněte na tlačítko **Nová politika**.
3. Nejprve zadejte název nové politiky, volitelně její popis. Klikněte na tlačítko **Pokračovat**.
4. Dále z rozbalovacího menu Produkt vyberte **ESET Endpoint for Windows**.
5. V **konfigurační šabloně** přejděte na záložku **Uživatelské rozhraní** > **Přístup k nastavení**.
6. V závislosti na verzi ESET Endpoint Security, kliknutím na přepínač aktivujte možnost **Chránit nastavení heslem**. Mějte na paměti, že ochrana heslem byla ve verzi 7 vylepšena. Pokud v síti používáte také starší verze produktů, nastavte pro každou verzi rozdílné heslo. Zadáním hesla pouze do pole pro produkt ve verzi 6 snížíte ochranu produktu ve verzi 7 a novější.
7. V zobrazeném oznámení zadejte požadované heslo a klikněte na tlačítko **OK**. Klikněte na tlačítko **Pokračovat**.
8. Dále vyberte klienty, na které chcete politiku aplikovat. Klikněte na tlačítko **Přiřadit…** vyberte konkrétní počítače nebo skupiny. Akci potvrďte kliknutím na tlačítko **OK**.
9. Ověřte, že jste vybrali všechny stanice, na které chcete politiku aplikovat, a klikněte na tlačítko **Pokračovat**.

10. Zkontrolujte, zda nastavení odpovídá vašim představám a pro vytvoření politiky klikněte na tlačítko **Dokončit**.

Co jsou to politiky?

Politiky představují účinný nástroj pro vzdálenou konfiguraci bezpečnostních produktů ESET a administrátorovi umožňují vynutit požadované nastavení z ESET PROTECT Web Console. Politiky může administrátor přiřazovat na skupiny nebo pouze konkrétní počítače. Na každou skupinu nebo počítač se může aplikovat více politik.

Pro vytváření a přiřazování politik počítačům a skupinám musí mít uživatel potřebné oprávnění: Pro zobrazení seznamu politik včetně jejich konfigurace přiřaďte uživateli oprávnění pro **čtení**. Pro přiřazení politiky konkrétnímu zařízení musí mít oprávnění **Použít**.

Politiky se aplikují v pořadí podle statických skupin. Výjimku tvoří dynamické skupiny, kdy se politiky aplikují v opačném pořadí (směrem od potomka k rodiči). Díky tomuto principu můžete vytvářet globální politiky pro statické skupiny a politiky se specifickým nastavením přiřazovat podskupinám. Pomocí příznaků jste schopni konkrétní nastavení produktu ESET Endpoint Security vynutit v globální politice a zajistit, že nastavení již nepřepíše žádná politika umístěná ve stromu níže. Princip aplikování politik na klienty je popsán v online uživatelské příručce k ESET PROTECT.

> Doporučujeme vytvářet politiky od obecných (například s nastavením aktualizace) a přiřazovat je globálním skupinám (ve stromu výše). Politiky se specifickým nastavením (například blokování výměnných médií) přiřazujte následně podskupinám nebo přímo konkrétním klientům. Důvodem je, že při slučování politik je nastavení dříve aplikované politiky přepsáno nastavením z později aplikované politiky (pokud není v politice řečeno jinak pomocí příznaku).

Sloučení politik

Výsledné nastavení, které se aplikuje na klienta, se získá sloučením všech aplikovaných politik. Politiky se slučují postupně (jedna po druhé). Při slučování politik obecně platí, že později aplikovaná politika přepíše nastavení definované v politice aplikované dříve. Toto chování můžete změnit pomocí příznaku jednotlivě u každého nastavení.

V případě seznamů (výjimek, pravidel firewallu, ...) se můžete při vytváření politik rozhodnout co se stane, pokud bude stejná položka definována ve více politikách. K dispozici máte tyto možnosti:

- **Nahradit** – tato možnost je použita jako výchozí a znamená, že každá později aplikovaná politika přepíše seznam položek definovaný v dříve aplikované politice.
- **Přidat na konec** – při použití této možnosti se seznam položek přidá k již existujícímu (z jiné politiky) a záznamy z něj se umístí na konec. Lokální seznam se přepíše.
- **Přidat na začátek** – při použití této možnosti se seznam položek přidá k již existujícímu a záznamy z něj se umístí na začátek (budou tedy nadřazeny ostatním položkám/pravidlům). Lokální seznam se přepíše.

ESET Endpoint Security podporuje slučování seznamů definovaných na lokální stanici se seznamy definovanými prostřednictvím politik. Standardně se seznamy (například webových stránek) definované na lokální stanici přepíší seznamy definovanými v politice. V případě potřeby můžete definovat způsob sloučení obou seznamů.

- tato ikonka představuje možnosti pro slučování politik.
- Tato ikonka představuje možnosti pro slučování lokálního nastavení s politikami.

Více informaci o slučování politik naleznete v online uživatelské příručce k ESET PROTECT, kde si můžete prohlédnout rovněž vzorové příklady.

Jak fungují příznaky?

Výsledné nastavení, které se aplikuje na klienta, se získá sloučením všech aplikovaných politik. Průběh slučování politik a tvorbu výsledného nastavení můžete ovlivnit prostřednictvím příznaků. Příznaky určují, zda a jakým způsobem se dané nastavení politikou propíše.

Každému nastavení v politice můžete přiřadit příznak. Prostřednictvím příznaku určíte, jak má politika dané nastavení zpracovat. K dispozici jsou tři příznaky:

Neaplikovat	Nastavení s tímto příznakem nebude v politice definováno. Uživatel jej může změnit, případně bude definováno jinou politikou (aplikovanou později).
Použít	Nastavení s příznakem **Použít** se aplikuje na klientskou stanici. Může být přepsáno politikou, která se aplikuje později. Po odeslání politiky s tímto příznakem na klientskou stanici dojde ke změně lokální konfigurace. Protože nastavení není vynuceno, můžete kdykoli změněno jinou politikou aplikovanou později.
Vynutit	Nastavení s příznakem **Vynutit** má nejvyšší prioritu a nemůže být přepsáno jinou politikou uplatňovanou později (**i v případě, že má stejný příznak**). To zajistí, že se nastavení nezmění ani po sloučení všech politik a nezmění jej ani uživatel. Po odeslání politiky s tímto příznakem na klientskou stanici dojde ke změně lokální konfigurace.

Scénář: *Administrator* chce *Filipovi* přidělit oprávnění pro vytváření i úpravu politik v jeho skupině a zároveň chce, aby Filip viděl politiky, které *Administrator* vytvořil. Politiky, které vytvořil Administrator, budou mít příznak Vynutit. V tomto příkladu si ukážeme, jak Filipovi přidělit oprávnění pro čtení všech politik, včetně těch, které vytvořil *Administrator*. Dále *Filipovi* přidělíme oprávnění pro vytváření politik v jeho domovské skupině San Diego.

Řešení:*Administrator* musí provést tyto kroky:

Vytvoření vlastní statické skupiny a přiřazení oprávnění

1. Vytvoří novou statickou skupinu s názvem *San Diego*.
2. Vytvoří novou sadu oprávnění s názvem *Politiky – Všechna zařízení – Filip*, ve které jako statickou skupinu nastaví *Všechna zařízení* a u položky **Politiky** nastaví oprávnění **Číst**. Toto oprávnění umožní Filipovi zobrazit si politiky, které vytvořil Administrator.
3. Vytvoří novou sadu oprávnění s názvem *Politiky Filipa*, ve které jako statickou skupinu nastaví *San Diego*. Dále u položky **Politiky** a **Skupiny a počítače** nastaví oprávnění **Zápis**. Toto oprávnění umožní Filipovi *vytvářet a upravovat politiky v jeho domovské skupině (*San Diego).
4. Vytvoří nového uživatele s názvem *Filip* a v sekci **Oprávnění** vybere výše vytvořené sady oprávnění.

Vytvoření politik

5. Vytvoří novou politiku s názvem *Všechna zařízení – Zapnout firewall*. V sekci **Nastavení** vybere z rozbalovacího menu **ESET Endpoint for Windows**. V konfigurační šabloně přejde do větve **Síťová ochrana** > **Firewall** > **Obecné** a u všech nastaví aplikuje příznak **Vynutit**. V sekci **Přiřadit** vybere skupinu *Všechna zařízení*.
6. Vytvoří novou politiku s názvem *Filipova skupina – Zapnout firewall*. V sekci **Nastavení** vybere z rozbalovacího menu **ESET Endpoint for Windows**. V konfigurační šabloně přejde do větve **Síťová ochrana** > **Firewall** > **Obecné** a u všech nastaví aplikuje příznak **Použít**. V sekci **Přiřadit** vybere skupinu *San Diego*.

Výsledek

Politiky, které vytvořil *Administrator* se aplikují jako první. Protože nastavení v těchto politikách mají příznak Vynutit, nebudou přepsána politikami, které se aplikují později. Následně se aplikují politiky vytvořené *Filipem*, ale jejich nastavení nepřepíše hodnoty vynucenou politikou, kterou vytvořil Administrator.

Pro zobrazení finálního pořadí politik přejděte v hlavním menu na záložku **Počítače** (případně **Další** > **Skupiny**). Vyberte skupinu **San Diego**, klikněte na konkrétní počítač a z kontextového menu vyberte možnost Zobrazit detaily. Následně přejděte na záložku **Konfigurace** > **Aplikované politiky**.

Instalace

ESET Endpoint Security můžete na stanici nasadit mnoha způsoby, bez ohledu na to, zda ji spravujete vzdáleně prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud.

Z ESET Endpoint Security se můžete vrátit k ESET Endpoint Antivirus spuštěním instalačního programu ESET Endpoint Antivirus s již nainstalovaným ESET Endpoint Security. Musíte však nainstalovat stejnou nebo novější verzi.

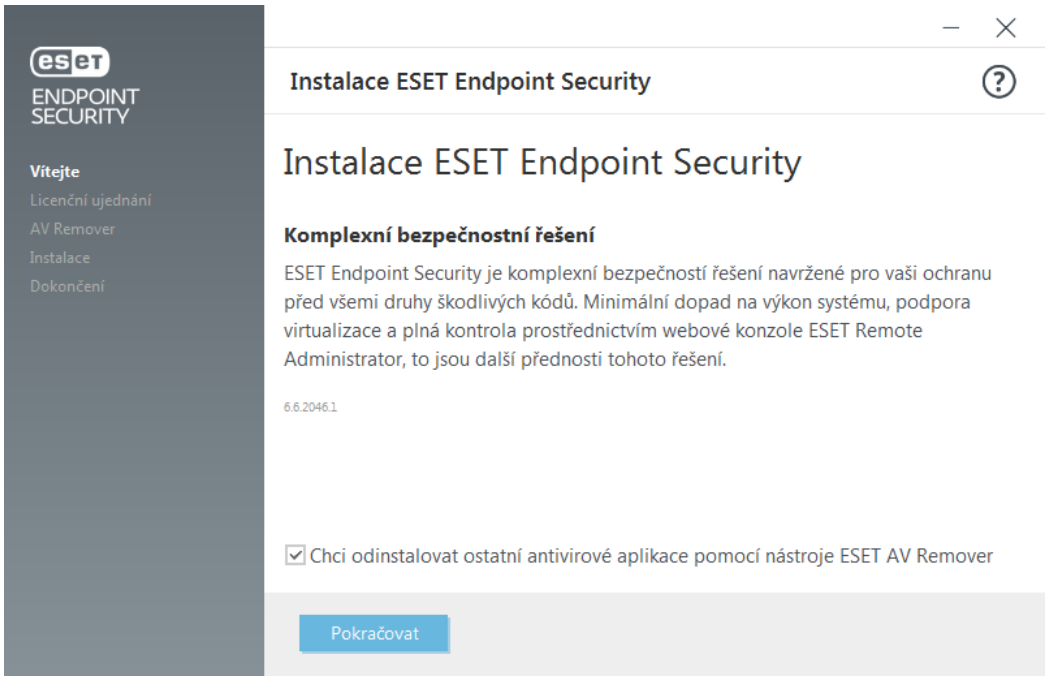
Způsob	Záměr	Odkaz ke stažení
Instalace včetně ESET AV Remover	Nástroj ESET AV Remover vám pomůže odstranit nejrozšířenější antivirové programy před zahájením samotné instalace produktu ESET.	Stáhnout 64bitovou verzi Stáhnout 32bitovou verzi
.exe balíček	Instalace bez spuštění ESET AV Remover.	Stáhnout 64bitovou verzi Stáhnout 32bitovou verzi

Způsob	Záměr	Odkaz ke stažení
Instalace (.msi)	Ve firemním prostředí je .msi preferovaný typ instalačního balíčku. Je to především z důvodu možnosti offline instalace a jeho vzdáleného nasazení prostřednictvím mnoha nástrojů jakým je mj. ESET PROTECT.	Stáhnout 64bitovou verzi Stáhnout 32bitovou verzi
Instalace z příkazového řádku	ESET Endpoint Security můžete nainstalovat lokálně prostřednictvím příkazového řádku nebo vzdáleně klientskou úlohou z ESET PROTECT.	N/A
Nasazení prostřednictvím GPO a SCCM	Použijte nástroje pro správu jako je GPO nebo SCCM pro nasazení ESET Management Agenta a ESET Endpoint Security na klientské stanice.	N/A
Nasazení pomocí RMM nástrojů	Prostřednictvím ESET DEM pluginů pro vzdálenou správu a monitorování (RMM) můžete na klientské stanici nasadit ESET Endpoint Security.	N/A

ESET Endpoint Security je dostupný ve více než 30 jazycích.

Instalace včetně ESET AV Remover

Je důležité, abyste před instalací produktu ESET odinstalovali jiné bezpečnostní aplikace, jejichž součástí jsou prvky rezidentní ochrany (například antivirové a antispywarové programy, firewall). Současné používání několika takových aplikací může vést k vážným konfliktům. Po spuštění instalace vyberte možnost **Chci odinstalovat ostatní antivirové aplikace pomocí nástroje ESET AV Remover**. Poté ESET AV Remover prohledá váš počítač a odstraní všechny podporované bezpečnostní aplikace. Pokud toto možnost nevyberete, bude **pokračovat** standardní instalace ESET Endpoint Security bez nástroje ESET AV Remover.

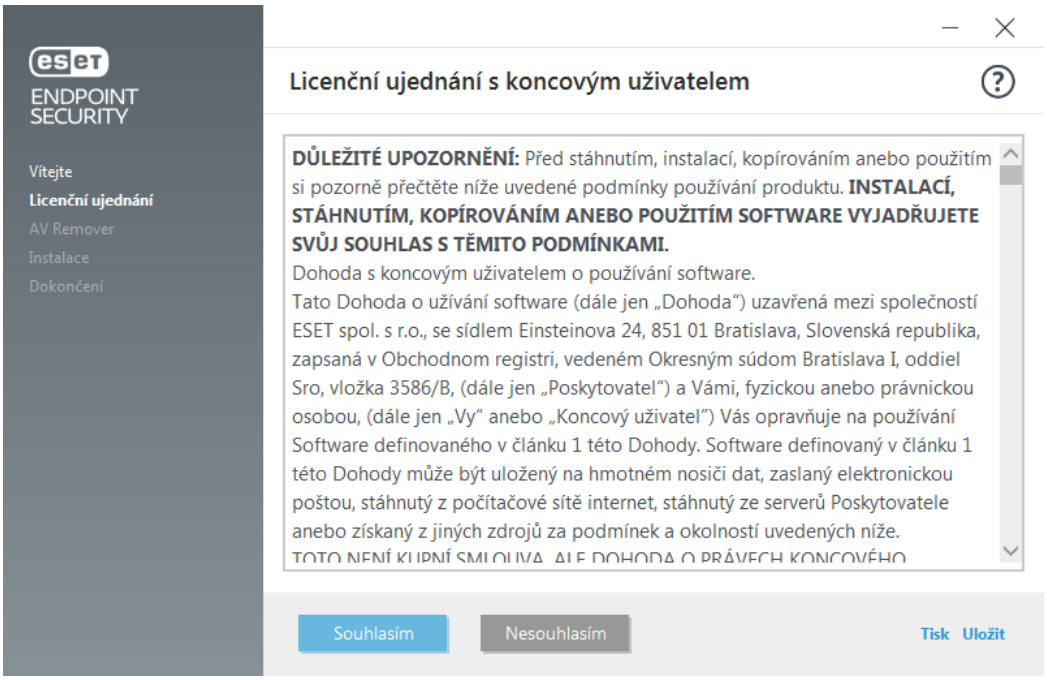


ESET AV Remover

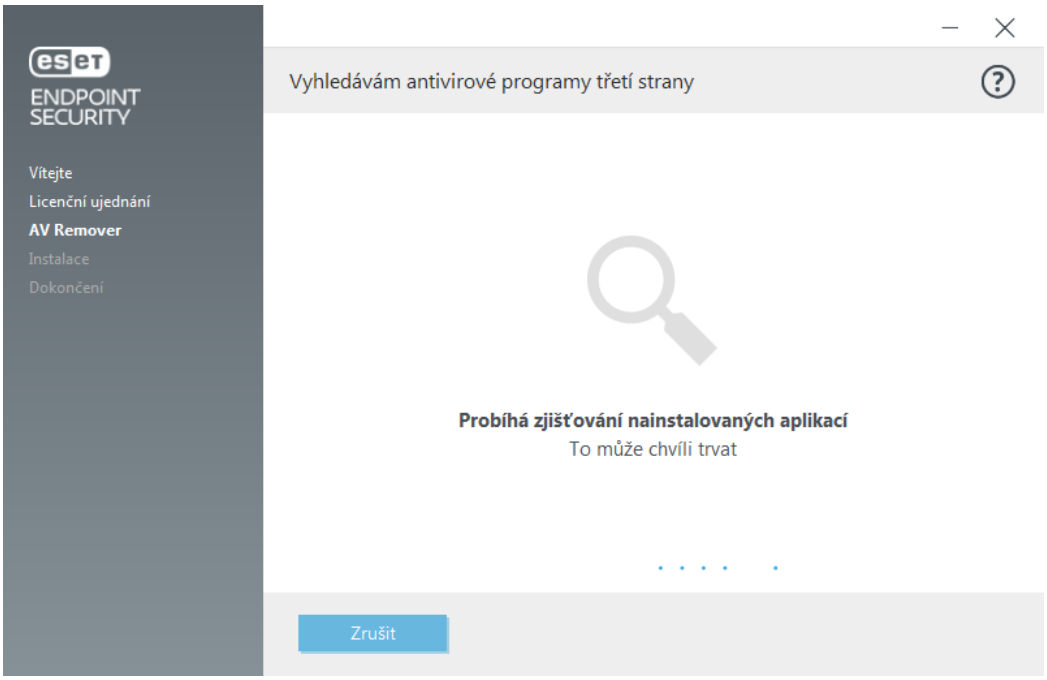
Nástroj ESET AV Remover vám pomůže ze systému odstranit nejrozšířenější antivirové programy. Podle následujících kroků odeberete stávající antivirový program z počítače pomocí ESET AV Remover:

1. Seznam aplikací, které ESET AV Remover podporuje, naleznete v ESET Databázi znalostí.

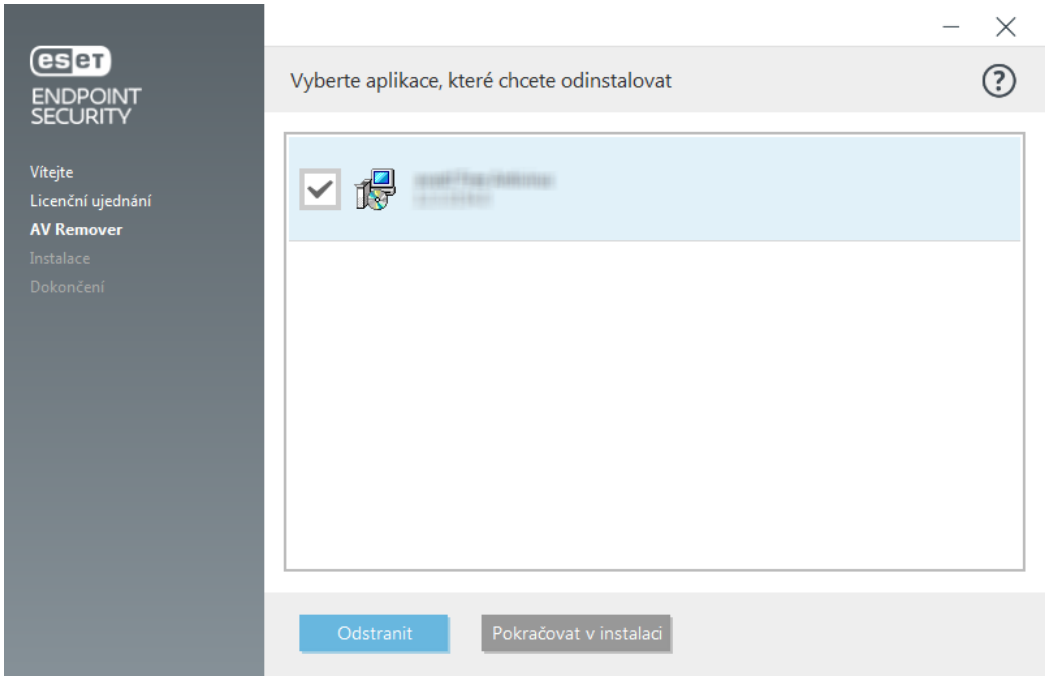
2. Po kliknutí na tlačítko **Přijmout** nástroj ESET AV Remover prohledá váš počítač. Pokud kliknete na **Nesouhlasím**, bude pokračovat instalace ESET Endpoint Security bez odebrání již existujících produktů v systému.



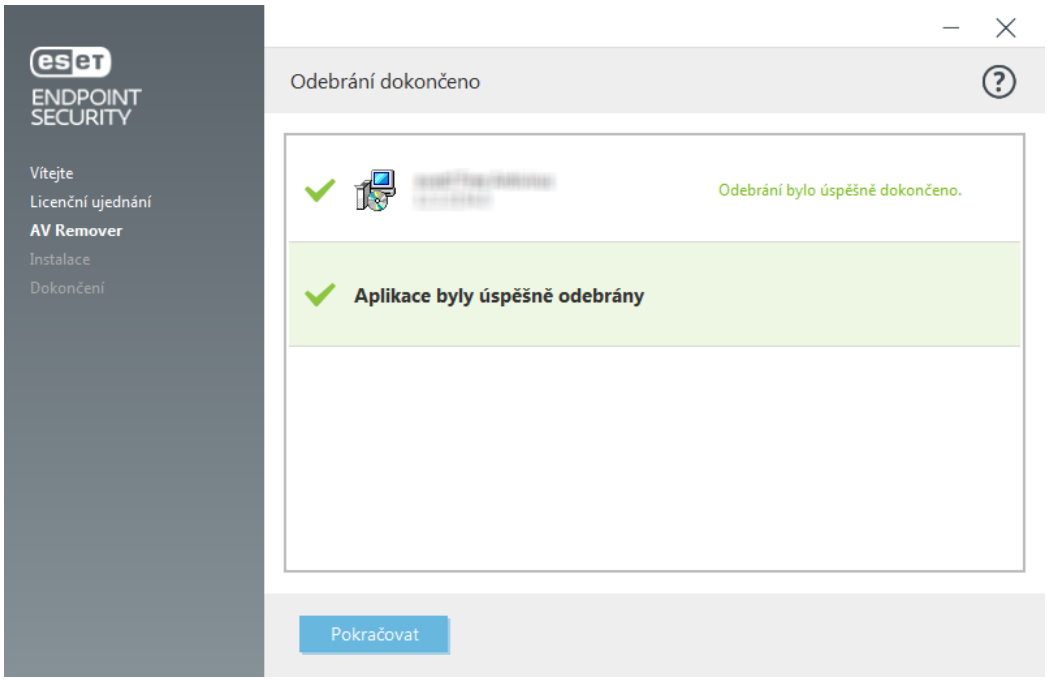
2. ESET AV Remover se pokusí ve vašem systému najít jiná antivirová řešení.



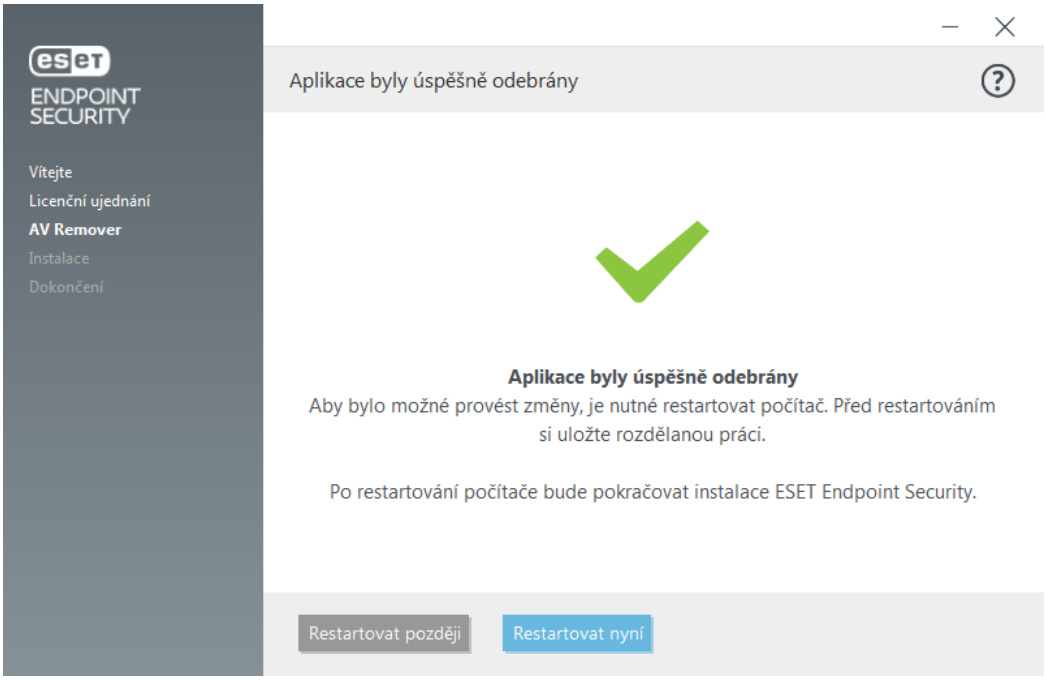
2. Vyberte aplikace, které chcete odebrat ze systému a klikněte na tlačítko **Odebrat**. Tato akce může chvíli trvat.



2. Po úspěšném odebrání klikněte na tlačítko **Pokračovat**.



6. Pro dokončení změn v systému restartujte počítač a poté pokračujte instalací ESET Endpoint Security. Pokud se odebrání nezdařilo, postupujte podle kroků uvedených v kapitole Odinstalace prostřednictvím ESET AV Remover skončila s chybou.



Odinstalace prostřednictvím ESET AV Remover skončila s chybou

Pokud se stávající antivirový program nepodaří odstranit, zobrazí upozornění, že odinstalace aplikace prostřednictvím ESET AV Remover není pravděpodobně podporována. V takovém případě bude nutné aplikaci odebrat ručně nebo použijte nástroje pro odstranění nejznámějších antivirových programů.

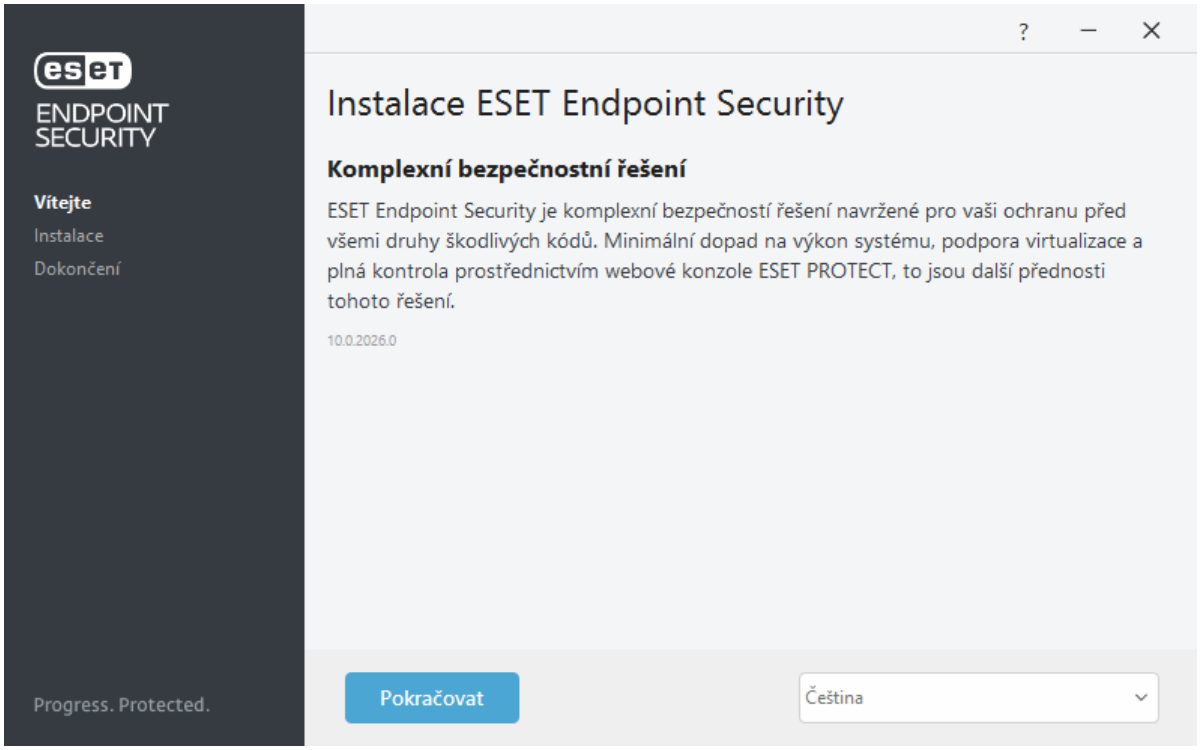
Při neúspěšné odinstalaci jiného bezpečnostního produktu mohly v systému zůstat jeho zbytky. Proto budete vyzváni k **restartování počítače a provedení nové kontroly** na přítomnost těchto pozůstatků. Proto budete vyzváni k restartování počítače a provedení nové kontroly na přítomnost těchto pozůstatků.

V případě přetrvávajících problémů s odinstalací jiných aplikací prostřednictvím nástroje ESET AV Remover kontaktujte technickou podporu ESET. Společně s popisem problému zašlete na technickou podporu soubor **AppRemover.log**. Soubor **AppRemover.log** naleznete ve složce **eset** , která se vytvoří v dočasné složce *%TEMP%*. Pro jeho získání použijte Průzkumníka Windows. Specialisté technické podpory společnosti ESET vás budou kontaktovat co nejdřív, aby vám pomohli vyřešit váš problém.

Instalace (.exe)

Po spuštění .exe instalačního balíčku se zobrazí průvodce, který vás provede celým procesem instalace.

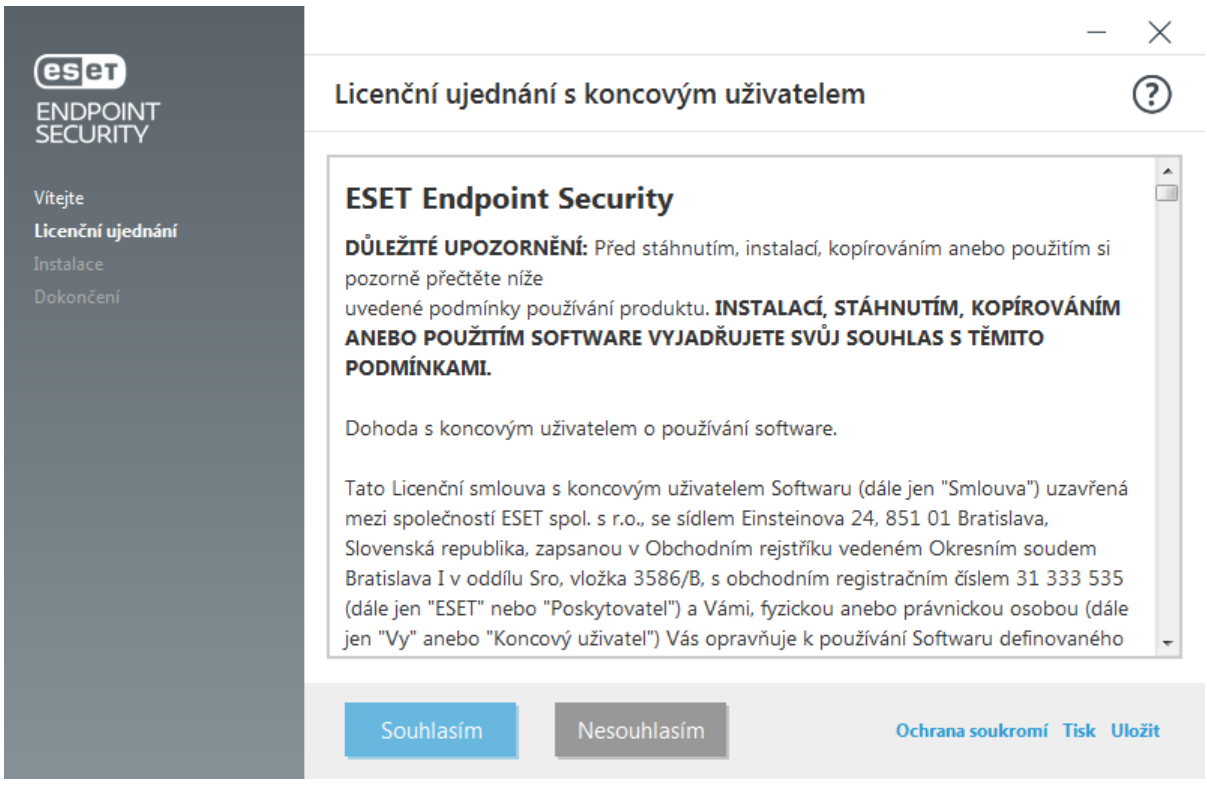
Ujistěte se, zda nemáte nainstalován další antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě. Proto doporučujeme odinstalovat všechny ostatní antivirové programy. V databázi znalostí naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů (dostupný v angličtině a několika dalších jazycích).



1. Vyberte, zda chcete využívat následující funkce, přečtěte si Licenční ujednání s koncovým uživatelem a Zásady ochrany osobních údajů. Klikněte na tlačítko **Pokračovat**, případně klikněte na **Povolit vše a pokračovat**, čímž zapnete funkce:

- Systém zpětné vazby ESET LiveGrid®
- Detekci potenciálně nechtěných aplikací

Kliknutím na tlačítko **Pokračovat** nebo **Povolit vše a pokračovat** souhlasíte se zněním Licenčního ujednání s koncovým uživatelem a berete na vědomí Zásady ochrany osobních údajů. Pokud chcete ESET Endpoint Security nainstalovat do jiné než výchozí složky, klikněte na Změnit instalační složkuPRODUCTNAME.



2. Po dokončení instalace budete vyzváni k aktivaci produktu ESET Endpoint Security.

Změna instalační složky (.exe)

V průběhu instalace můžete **Změnit instalační složku**. Po vybrání možnosti vyberte složku umístění instalace ESET Endpoint Security. Standardně se program instalujte do následující složky:

C:\Program Files\ESET\ESET Security

Definovat můžete také složku pro uložení programových komponent a dat programu. Standardně se instalují do následujících složek:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Pro změnu cílového umístění klikněte na tlačítko **Procházet…** (nedoporučujeme).

Klikněte na tlačítko **Zpět** a pokračujte v procesu instalace.

Instalace (.msi)

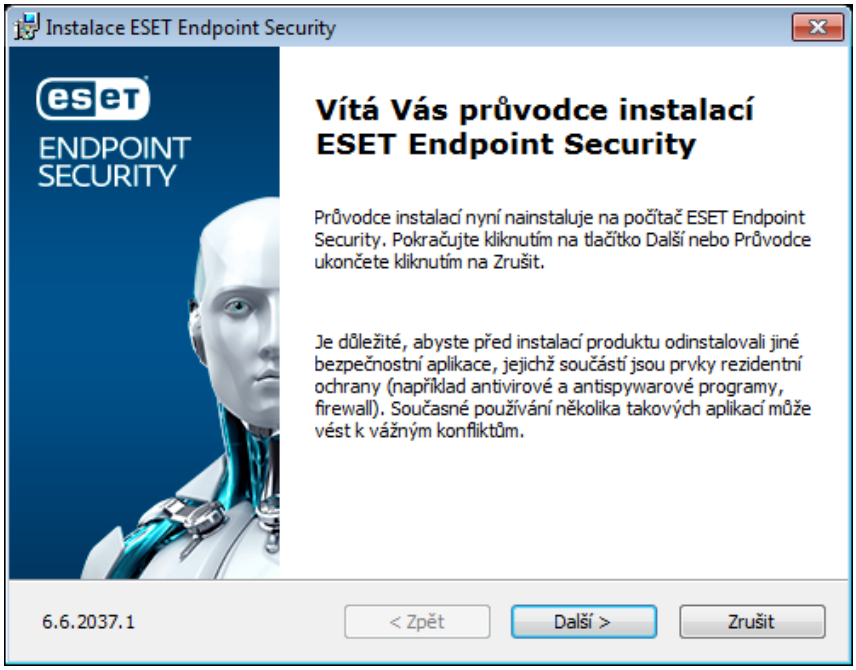
Po spuštění .msi instalačního balíčku se zobrazí průvodce, který vás provede celým procesem instalace.

Ve firemním prostředí je .msi preferovaný typ instalačního balíčku. Je to především z důvodu možnosti offline instalace a jeho vzdáleného nasazení prostřednictvím mnoha nástrojů jakým je mj. ESET PROTECT.

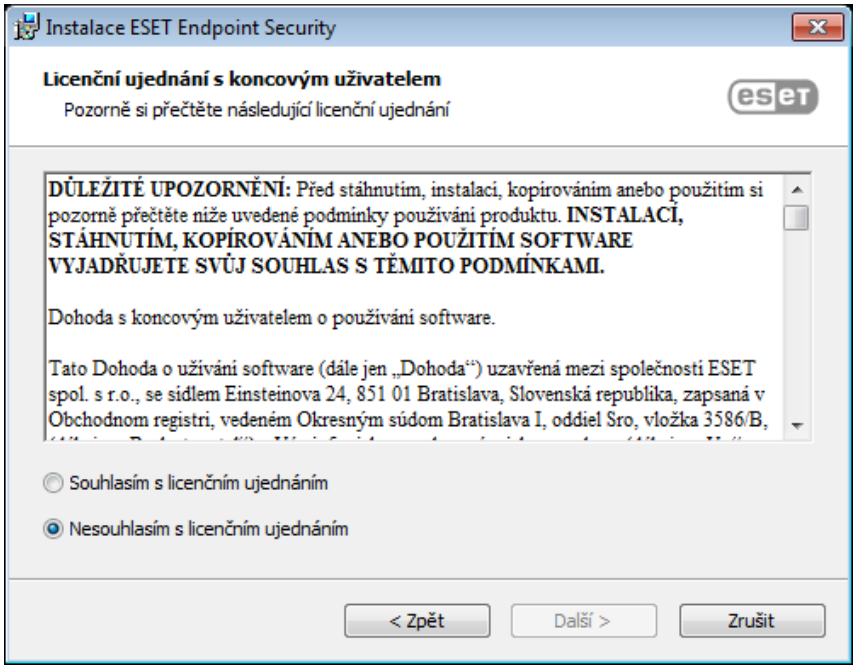
Ujistěte se, zda nemáte nainstalován další antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě. Proto doporučujeme odinstalovat všechny ostatní antivirové programy. V databázi znalostí naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů (dostupný v angličtině a několika dalších jazycích).

Instalační balíček ESET Endpoint Security vytvořený pomocí ESET PROTECT podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 v režimu více relací.

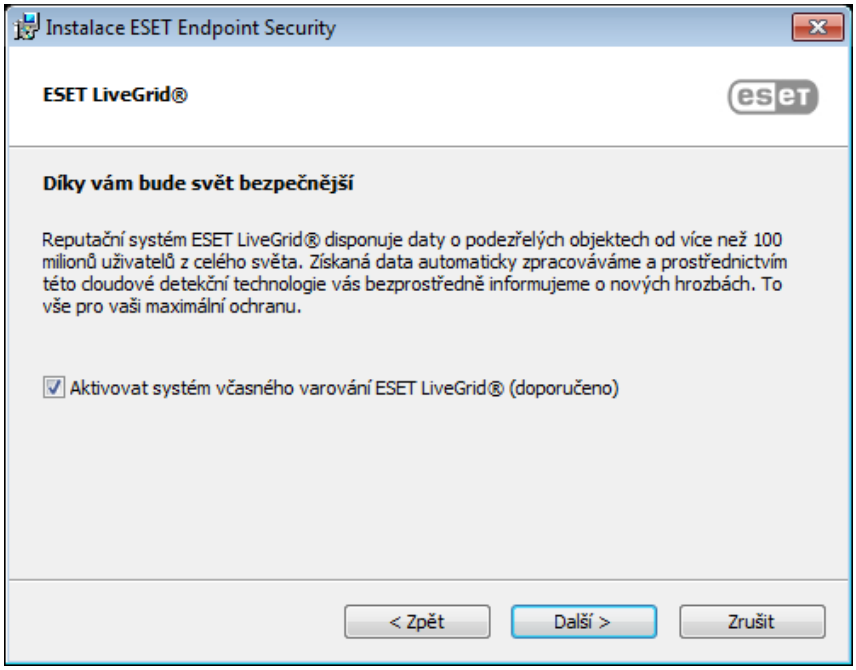
1. Vyberte si požadovaný jazyk a klikněte na tlačítko **Další**.



2. V dalším kroku se zobrazí licenční ujednání s koncovým uživatelem. Přečtěte si jej a kliknutím na **Přijmout** jej odsouhlaste. V instalaci pokračujte kliknutím na tlačítko **Další**.



3. Dále se rozhodněte, zda chcete zapnout systém zpětné vazby ESET LiveGrid®. ESET LiveGrid® pomáhá bezprostředně informovat společnost ESET o nových hrozbách a tím chránit zákazníky. Tento systém funguje na principu odeslání podezřelých vzorků do virové laboratoře společnosti ESET, kde jsou analyzovány a využívány při vytváření detekčního jádra. Pokud chcete **konfigurovat další instalační parametry**, klikněte na Pokročilá nastavení.



4. Kliknutím na tlačítko **Instalovat** zahájíte instalaci produktu. Po dokončení instalace budete vyzváni k aktivaci produktu ESET Endpoint Security.

Pokročilá instalace (.msi balíček)

Pokročilý režim instalace vám umožňuje přizpůsobit parametry instalace, které nejsou dostupné ve standardním režimu instalace.

1. V průběhu instalace můžete **Změnit instalační složku**. Po vybrání možnosti vyberte složku umístění instalace ESET Endpoint Security. Ve výchozím nastavení se program instaluje do následujících složek:

C:\Program Files\ESET\ESET Security

Definovat můžete také složku pro uložení programových komponent a dat programu. Standardně se instalují do následujících složek:

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

Pro změnu cílového umístění klikněte na tlačítko **Procházet…** (nedoporučujeme).

2. Vyberte, které součásti produktu chcete nainstalovat. Můžete si vybrat, jakou kontrolu počítače chcete provádět a všechny dostupné ochrany. Mirror můžete použít pro aktualizaci dalších počítačů ve vaší síti. Remote Monitoring and Management (RMM) je způsob pro vzdálené monitorování a ovládání aplikací prostřednictvím lokálně nainstalovaného agenta poskytnutého MSP (Managed Service Provider).
3. Kliknutím na tlačítko **Instalovat** spustíte instalaci.

Minimální instalace

Za účelem snížení množství přenášených dat souvisejících s instalačním balíčkem produktu a úspory prostředků nabízíme instalační balíček obsahující minimum potřebných modulů. Instalační balíček obsahuje pouze nejdůležitější moduly pro zajištění funkčnosti a všechny ostatní moduly se stáhnou v průběhu prvotní aktualizace

produktu, která proběhne po jeho aktivaci. Výhodou tohoto řešení je výrazné snížení velikosti instalačního balíčku.

Instalační balíček pro režim v minimální instalaci obsahuje následující moduly:

- Loader
- Modul Direct Cloud komunikace
- Modul jazykové lokalizace
- Konfigurace
- SSL

Po aktivaci produktu se zobrazí stav hlášení **Probíhá inicializace ochrany**, které vás informuje o tom, že probíhá prvotní konfigurace funkcí.

V případě problému se stahováním modulů (například z důvodu chybného nastavení proxy, nedostupné sítě, atd.) se stav aplikace změní na oranžový a zobrazí se hlášení **Je vyžadována vaše pozornost**. Po vyřešení problému s konektivitou přejděte v hlavním okně programu na záložku **Aktualizace** a pro zahájení procesu aktualizace klikněte na možnost **Zkontrolovat aktualizace**.

Po několika neúspěšných pokusech se stav aplikace změní na červenou a zobrazí se hlášení **Ochranu se nepodařilo nastavit**. Pro opětovný pokus nastavení ochrany klikněte na možnost Zkusit znovu. V případě, že dojde k selhání inicializačního procesu a nejste schopni stáhnout zbývající moduly, použije úplný MSI instalační balíček.

Pokud stanice nemá přístup k internetu, případně je v offline prostředí, pro její aktualizaci využijte jedno z následujících řešení, které bude zajišťovat stahování aktualizačních souborů ze serverů ESET:
- Aktualizace z mirroru
- Použití Mirror Toolu

Instalace z příkazového řádku

ESET Endpoint Security můžete nainstalovat lokálně prostřednictvím příkazového řádku nebo vzdáleně klientskou úlohou z ESET PROTECT.

Podporované parametry

APPDIR=<path>

- Cesta – platná cesta ke složce.
- Složka, do které se aplikace nainstaluje.

APPDATADIR=<path>

- Cesta – platná cesta ke složce.
- Složka, do které se nainstalují datové soubory aplikace.

MODULEDIR=<path>

- Cesta – platná cesta ke složce.
- Složka, do které se nainstalují moduly aplikace.

ADDLOCAL=<list>

- Komponenty k instalaci – seznam volitelných funkcí, které je možné nainstalovat.
- Příklad použití .msi balíčku: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Pro více informací o vlastnosti **ADDLOCAL** přejděte do databáze znalostí společnosti Microsoft: http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- ADDEXCLUDE je seznam funkcí oddělených čárkou, které nechcete nainstalovat. Jedná se o náhradu staré vlastnosti REMOVE.
- Po vybrání funkce, kterou nechcete instalovat, je nutné definovat úplnou cestu (včetně jejich podfunkcí) a související neviditelné funkce.
- Příklad použití .msi balíčku: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> Parametr **ADDEXCLUDE** nemůžete použít společně s parametrem **ADDLOCAL**.

Pro více informací, jaké přepínače podporuje konkrétní verze **msiexec** se podívejte do dokumentace Windows Installeru.

Pravidla

- **ADDLOCAL** je seznam funkcí oddělených čárkou, které chcete nainstalovat.
- Po vybrání podřízené komponenty musíte specifikovat také nadřazenou komponentu.
- Pro správné použití si prohlédněte sekci Další pravidla, kterou naleznete níže.

Komponenty a funkce

> Instalace komponent prostřednictvím vlastnosti ADDLOCAL/ADDEXCLUDE nefunguje pro ESET Endpoint Antivirus.

Funkce jsou rozděleny do čtyř kategorií:

- **Povinná** – tato komponenta musí být vždy nainstalována.
- **Volitelná** – instalaci těchto komponent můžete zrušit.
- **Neviditelná** – logická součást, která je povinná pro fungování jiných funkcí.
- **Rozcestník** – součást, která nemá vliv na produkt, ale musí být v seznamu podfunkcí uvedena.

Níže uvádíme seznam komponent produktu ESET Endpoint Security:

Popis	Název komponenty	Nadřazená komponenta	Přítomnost
Základní komponenty programu	`Computer`		Rozcestník
Detekční jádro	`Antivirus`	`Computer`	Povinná
detekční jádro / Detekce škodlivého kódu	`Scan`	`Computer`	Povinná
Detekční jádro / Rezidentní ochrana souborového systému	`RealtimeProtection`	`Computer`	Povinná
Detekční jádro / Detekce škodlivého kódu / Ochrana dokumentů	`DocumentProtection`	`Antivirus`	Volitelná

Popis	Název komponenty	Nadřazená komponenta	Přítomnost
Správa zařízení	DeviceControl	Computer	Volitelná
Síťová ochrana	Network		Rozcestník
Síťová ochrana / Firewall	Firewall	Network	Volitelná
Síťová ochrana / Ochrana proti síťovým útokům / …	IdsAndBotnetProtection	Network	Volitelná
Zabezpečený prohlížeč	OnlinePaymentProtection	WebAndEmail	Volitelná
Web a mail	WebAndEmail		Rozcestník
Web a mail / Filtrování protokolů	ProtocolFiltering	WebAndEmail	Neviditelná
Web a mail / Ochrana přístupu na web	WebAccessProtection	WebAndEmail	Volitelná
Web a mail / Ochrana poštovních klientů	EmailClientProtection	WebAndEmail	Volitelná
Web a mail / Ochrana poštovních klientů / Poštovní klienti	MailPlugins	EmailClientProtection	Neviditelná
Web a mail / Ochrana poštovních klientů / Antispamová ochrana poštovních klientů	Antispam	EmailClientProtection	Volitelná
Web a mail / Filtrování obsahu webu	WebControl	WebAndEmail	Volitelná
Nástroje / ESET RMM	Rmm		Volitelná
Aktualizace / Profily / Aktualizační mirror	UpdateMirror		Volitelná
ESET Inspect plugin	EnterpriseInspector		Neviditelná

Skupiny funkcí:

Popis	Název komponenty	Vyžadováno
Všechny povinné funkce	_Base	Neviditelná
Všechny dostupné funkce	ALL	Neviditelná

Další pravidla

- Pokud se rozhodnete pro jakoukoli součást **WebAndEmail**, je nutné specifikovat také neviditelnou položku **ProtocolFiltering**.
- V názvech funkcí se rozlišuje velikost písmen. UpdateMirror není to samé jako UPDATEMIRROR.

Seznam vlastností konfigurace

Vlastnost	Hodnota	Funkce
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – Vypnuto 1 – Zapnuto	Detekce potenciálně nechtěných aplikací (PUA)
CFG_LIVEGRID_ENABLED=	Viz níže	Podívejte se níže na vlastnost LiveGrid
FIRSTSCAN_ENABLE=	0 – Vypnuto 1 – Zapnuto	Naplánovat a spustit Kontrolu počítače po dokončení instalace.
CFG_PROXY_ENABLED=	0 – Vypnuto 1 – Zapnuto	Nastavení proxy serveru

Vlastnost	Hodnota	Funkce
CFG_PROXY_ADDRESS=	<ip>	IP adresa proxy serveru
CFG_PROXY_PORT=	<port>	Port, na kterém poslouchá proxy server
CFG_PROXY_USERNAME=	<username>	Uživatelské jméno pro autentifikaci
CFG_PROXY_PASSWORD=	<password>	Heslo pro autentifikaci
ACTIVATION_DATA=	Viz níže	Aktivace produktu licenčním klíčem nebo offline licenčním souborem
ACTIVATION_DLG_SUPPRESS=	0 – Vypnuto 1 – Zapnuto	Pokud nastavíte "1", nezobrazí se při prvním spuštění dialogové okno pro aktivaci produktu.
ADMINCFG=	<path>	Cesta k exportované konfiguraci ve formátu XML (výchozí hodnota: *cfg.xml*)

Vlastnosti dostupné pouze v ESET Endpoint Security

CFG_EPFW_MODE=	0 – Automatický (standardní) 1 – Interaktivní 2 – Administrátorský 3 – Učící	Režim filtrování firewallu
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Konec učícího režimu definovaný v unixovém čase

Vlastnost LiveGrid®

Pokud při instalaci ESET Endpoint Security použijete parametr CFG_LIVEGRID_ENABLED, výsledné nastavení produktu bude:

Funkce	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Reputační systém ESET LiveGrid®	Zapnuto	Zapnuto
Systém zpětné vazby ESET LiveGrid®	Vypnuto	Zapnuto
Odesílat anonymní statistiky	Vypnuto	Zapnuto

Vlastnost ACTIVATION_DATA

Formát	Způsob
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Aktivace prostřednictvím ESET licenčního klíče (vyžadováno připojení k internetu)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Aktivovali prostřednictvím offline licenčního souboru

Vlastnost jazyka

Jazyk ESET Endpoint Security (definovat je nutné oba parametry)

Vlastnost	Hodnota
PRODUCT_LANG=	LCID desítkové číslo (Locale ID). Například 1029 pro češtinu. Více informací si přečtěte v kapitole Podporované jazyky.

Vlastnost	Hodnota
PRODUCT_LANG_CODE=	LCID řetězec (Language Culture Name) uvedený malými písmeny. Například cs-cz pro češtinu. Více informací si přečtěte v kapitole Podporované jazyky.

Vlastnosti restartování počítače

Následující parametry můžete použít pro restartování počítače po dokončení instalace:

Vlastnost	Hodnota	Funkce
REBOOT_WHEN_NEEDED=	0 – Vypnuto 1 – Zapnuto	Pokud je tato možnost zapnutá, po dokončení instalace se počítač restartuje.
REBOOT_CANCELABLE=	0 – Vypnuto 1 – Zapnuto	Pokud je tato možnost zapnutá, uživatel bude schopen zrušit restartování počítače.
REBOOT_POSTPONE=	hodnota v sekundách	Maximální doba v sekundách, po kterou může uživatel odložit restartování počítače.

Hodnoty REBOOT_CANCELABLE a REBOOT_POSTPONE se berou v potaz pouze v případě, kdy je povolen REBOOT_WHEN_NEEDED.

Příklady instalace z příkazového řádku

Před instalací se ujistěte, že jste si přečetli Licenční ujednání s koncovým uživatelem a máte oprávnění administrátora.

Odebrání **NetworkProtection** (definovat je nutné také všechny potomky):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Pokud chcete produkt ESET Endpoint Security automaticky nakonfigurovat po dokončení instalace, použijte v instalačním příkazu základní konfigurační parametry.
Instalace ESET Endpoint Security se zapnutou funkcí ESET LiveGrid®:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Instalace do jiné, než výchozí složky:
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Instalace a aktivace ESET Endpoint Security prostřednictvím ESET licenčního klíče.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Tichá instalace s detailním protokolováním (užitečné při řešení problémů), RMM a pouze povinných komponent:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Vynucená tichá instalace v konkrétním jazyce.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Možnosti pro ovládání produktu prostřednictvím příkazového řádku

- ESET CMD – slouží k importování .xml konfiguračního souboru a zapínání/vypínání bezpečnostních funkcí
- Skener příkazového řádku – slouží pro spuštění kontroly počítače

Nasazení prostřednictvím GPO a SCCM

ESET Endpoint Security můžete na stanici nainstalovat ručně, stejně tak pro jeho distribuci lze využít doménovou politiku (GPO) nebo nástroje určené pro hromadné nasazení aplikací, například SCCM, Symantec Altiris nebo Puppet.

Spravované prostředí (doporučeno)

Ve spravovaných prostředích doporučujeme nejprve na stanici nasadit ESET Management Agenta a následně prostřednictvím ESET PROTECT nainstalovat bezpečnostní produkt ESET Endpoint Security. ESET PROTECT musíte mít již v tomto případě ve své síti nasazen.

1. Stáhněte si samostatný instalační balíček ESET Management Agenta.
2. Připravte si GPO/SCCM skript.
3. Nasaďte ESET Management Agenta prostřednictvím GPO nebo SCCM.
4. Ověřte, že se stanice připojuje k ESET PROTECT.
5. Na stanici nasaďte a aktivujte ESET Endpoint Security.

Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
- Nasazení ESET Management Agenta prostřednictvím SCCM nebo GPO
- Nasazení ESET Management Agenta prostřednictvím Objektu zásad skupin (GPO)

Nespravované prostředí

Na stanice, které centrálně nespravujete nasaďte ESET Endpoint Security přímo. Nicméně nejedná se o doporučený způsob, protože nemáte k dispozici přehled o stavu produktu a nemůžete na něj prostřednictvím politik vynutit požadované nastavení.

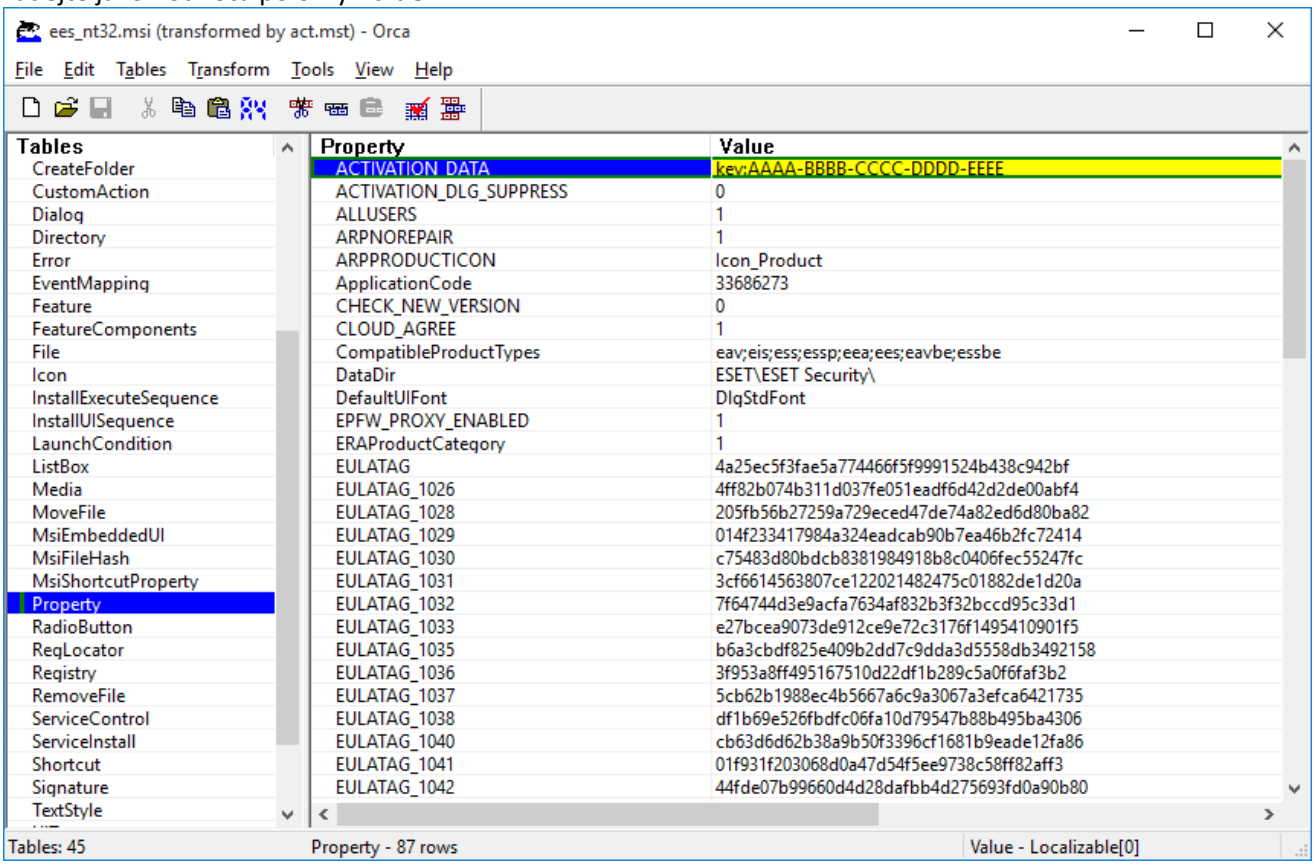
Po dokončení instalace není produkt ESET Endpoint Security standardně aktivován a funkční.

Možnost 1 (Instalace aplikace)

1. Stáhněte si .msi instalační balíček produktu ESET Endpoint Security.
2. Z .msi balíčku si vytvořte .mst transformaci (například pomocí nástroje Orca) a přidejte do ní vlastnost pro aktivaci produktu (viz `ACTIVATION_DATA` v kapitole Instalace z příkazového řádku)

Zobrazit kroky pro vytvoření .mst v nástroji Orca

1. Otevřete Orca.
2. Kliknutím na **File** > **Open** načtěte .msi instalační balíček.
3. Klikněte na **Transform** > **New Transform**.
4. V sekci **Tables** klikněte na **Property** a následně v hlavním menu na **Tables** > **Add row**.
5. V dialogovém okně **Add Row** zadejte ACTIVATION_DATA jako hodnotu položky **Property** a licenční informace zadejte jako hodnotu položky **Value**.



6. Klikněte na **Transform** > **Generate Transform** a uložte si .mst soubor.

1. Volitelné: Pro importování vámi požadované konfigurace do produktu ESET Endpoint Security prostřednictvím .xml souboru (například pro aktivaci RMM nebo nastavení proxy serveru) umístěte soubor cfg.xml do stejné složky jako instalační .msi balíček.
2. Nasaďte na stanici .msi instalační balíček společně s .mst souborem vzdáleně prostřednictvím GPO (viz Instalace aplikace) nebo SCCM.

Možnost 2 (prostřednictvím naplánované úlohy)

1. Stáhněte si .msi instalační balíček produktu ESET Endpoint Security.
2. Připravte si skript pro Instalaci z příkazového řádku, který bude obsahovat informace pro aktivaci produktu (viz `ACTIVATION_DATA`)
3. Ujistěte se, že je .msi instalační balíček a .cmd skript dosažitelný ze všech stanic ve vaší síti.
4. Volitelné: Pro importování vámi požadované konfigurace do produktu ESET Endpoint Security prostřednictvím .xml souboru (například pro aktivaci RMM nebo nastavení proxy serveru) umístěte soubor cfg.xml do stejné složky jako instalační .msi balíček.
5. Připravený skript pro instalaci použijte prostřednictvím GPO nebo SCCM.

    - V případě GPO použijte Group Policy Preferences > Group Policy Schedule Tasks > Immediate task.

Pokud pro vzdálenou správu bezpečnostních produktů ESET nechcete využít ESET PROTECT, ESET Endpoint Security obsahuje ESET plugin pro RMM, díky němuž můžete na produkt dohlížet a spravovat jej prostřednictvím lokálně nainstalovaného agenta poskytnutého MSP (Managed Service Provider). Více informací

Aktualizace na novou verzi

Nové verze ESET Endpoint Security opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů.

Existuje několik způsobů, jak aktualizovat produkt na novější verzi:

1. Automatizovaně prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud.
2. Automaticky prostřednictvím GPO nebo SCCM.
3. Automaticky prostřednictvím aktualizace programu.
   Jelikož se aktualizace programu týká všech uživatelů a může mít významný dopad na systém, je vydávána až po dlouhém období testování na všech operačních systémech v různých konfiguracích. Pokud chcete aktualizovat na nejnovější verzi ihned po jejím vydání, použijte některou z níže uvedených metod.
   Ujistěte se, že máte v Rozšířených nastaveních > **Aktualizace** > **Profily** > **Aktualizace produktu** aktivní možnost **Režim aktualizace**.
4. Ručně, stažením instalačního balíčku z webových stránek společnosti ESET a nainstalováním nejnovější verze přes stávající.

Doporučené aktualizační scénáře

Spravuji nebo chci produkty ESET spravovat vzdáleně

Pokud spravujete více než 10 ESET Endpoint produktů, zvažte jejich aktualizaci prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud. Více se přečtěte v následujících kapitolách:

- ESET PROTECT | Aktualizace ESET aplikace prostřednictvím klientské úlohy
- ESET PROTECT | Příručka pro SMB s nejvýše 250 produkty z řady ESET Endpoint na platformě Windows
- Představení ESET PROTECT Cloud

Ruční aktualizace na klientské stanici

ESET Endpoint Security na klientské stanici aktualizujete ručně podle následujících kroků:

1. Ověřte, zda je aktuálně nainstalovaná verze podporována.
2. Ověřte, zda máte podporovaný operační systém.

2. Stáhněte si a nainstalujte nejnovější verzi přes stávající.

V případě verzí produktů, které již dosáhly konce svého životního cyklu, není garantována úspěšná instalace nejnovější verze přes předchozí verzi. Pro zjištění, zda je vámi používaná verze produktu ESET Endpoint Security podporována se podívejte do dokumentu popisujícípolitiku pro životní cyklus produktu.
Pokud používáte nepodporovanou verzi produktu ESET Endpoint Security, před přechodem na novou verzi jej nejprve odinstalujte. Další informace a návod popisující ruční aktualizaci produktu ESET Endpoint Security na klientské stanici krok za krokem naleznete v ESET Databázi znalostí.

Automatická aktualizace starších produktů

Vámi používaná verze produktu ESET již není podporována, a proto byl váš produkt aktualizován na nejnovější verzi.

Známé problémy při instalaci

Každá nová verze produktu ESET opravuje chyby a vylepšuje funkce. Stávající zákazníci s platnou licencí mohou svůj produkt ESET aktualizovat na nejnovější verze zcela zdarma.

Pro dokončení instalace postupujte podle následujících kroků:

1. Klikněte na tlačítko **Přijmout a pokračovat** pro souhlas s Licenčním ujednáním s koncovým uživatelem a Zásadami ochrany osobních údajů. Pokud nesouhlasíte s Licenčním ujednáním s koncovým uživatelem, klikněte na tlačítko **Odinstalovat**. Upozorňujeme, že tím ovšem není možný návrat k předešlé verzi produktu.
2. Klikněte na tlačítko **Přijmout vše a pokračovat** pro aktivování systému zpětné vazby ESET LiveGrid®. Pokud se nechcete do uvedeného systému zapojit, klikněte na tlačítko **Pokračovat**.
3. Po automatické aktivaci produktu ESET licenčním klíčem se zobrazí domovská obrazovka programu. Pokud program nenalezne vaše licenční údaje, pokračujte aktivací zkušební licence. Jestliže licence použitá v předchozím produktu není platná, aktivujte produkt vámi zakoupenou licencí.
4. Pro úplné dokončení instalace je vyžadován restart.

Aktualizace zajišťující bezpečnost a stabilitu

Pravidelná aktualizace produktu ESET Endpoint Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Každá nová verze ESET Endpoint Security přináší mnoho vylepšení a opravuje chyby. Důrazně doporučujeme pravidelně aktualizovat ESET Endpoint Security, abyste si zajistili ochranu před hrozbami a eliminovali možnost zneužití bezpečnostních zranitelností. Na ESET Endpoint Security, stejně jako další produkty ESET, se vztahuje životní cyklus produktu.

Více informací naleznete v:
Databázi znalostí v článku End of Life policy (Business products)
Aktualizace produktu
Hotfixy zajišťující bezpečnost a stabilitu
Pro více informací týkajících se této změny v produktu ESET Endpoint Security přejděte do Databáze znalostí.

Automatické aktualizace jsou důležité pro zajištění maximální bezpečnosti a stability vámi používaného produktu. Z tohoto důvodu není možné aktualizace zajišťující bezpečnost a stabilitu deaktivovat.

Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu.

Produkt můžete aktivovat několika způsoby. Dostupnost jednotlivých metod závisí na zvoleném aktivačním scénáři a může se lišit v jednotlivých zemích a způsobu distribuce (webové stránky společnosti ESET, .exe nebo .msi instalační balíček apod.).

Aktivaci ESET Endpoint Security proveďte v hlavním okně programu > **Nápověda a podpora** a klikněte na tlačítko **Aktivovat produkt** nebo **Stav ochrany** > **Aktivovat produkt**.

ESET Endpoint Security můžete aktivovat níže uvedenými způsoby:

- **Použít zakoupený licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a aktivaci.
- **ESET HUB** – ESET HUB účet, který musíte vytvořit. ESET HUB je centrální bránou k jednotné bezpečnostní platformě ESET PROTECT. Poskytuje centralizovanou správu identit, předplatného a uživatelů pro všechny moduly platformy ESET. Pomocí této volby můžete aktivovat ESET Endpoint Security také pomocí starších nástrojů pro správu licencí: ESET Business Account nebo ESET MSP Administrator.
- **Offline licenční soubor** – automaticky generovaný soubor obsahující informace o licenci. Pokud to vaše licence umožňuje, offline licenční soubor si můžete vygenerovat na licenčním portále použít jej pro aktivaci stanic, které nejsou připojeny k internetu a není možné je aktivovat jiným způsobem. Počet offline licencí se odečte od celkového počtu dostupných licencí. Další informace o generování offline licenčních souborů najdete v online uživatelské příručce k ESET Business Account.

Možnost **Aktivovat později** použijte v případě, že je počítač připojen k internetu a vzdáleně spravován prostřednictvím ESET PROTECT. Tuto možnost můžete použít také v případě, kdy chcete klienta aktivovat později jiným způsobem.

Pokud máte pouze klasické licenční údaje (uživatelské jméno a heslo) pro aktivaci starších produktů ESET, převeďte si je nejprve na licenční klíč.

Licenci produktu můžete kdykoli změnit v hlavním okně programu > **Nápověda a podpora** > **Změnit licenci**. Na této obrazovce zároveň naleznete veřejné ID licence, které se používá pro identifikaci uživatele při komunikaci s technickou podporou společnosti ESET.

> Prostřednictvím ESET PROTECT můžete aktivovat produkt vzdáleně a plně automaticky. Pokyny naleznete v online nápověděESET PROTECT.

Neúspěšná aktivace?

Zadání licenčního klíče během aktivace

Pro správný chod bezpečnostního produktu ESET Endpoint Security je důležité, aby byl automaticky aktualizován. To je možné pouze tehdy, pokud jste jej aktivovali pomocí **Licenčního klíče**.

Pokud po dokončení instalace nezadáte licenční klíč, produkt nebude aktivovaný. Licenci změníte v hlavním okně programu. Na záložce **Nápověda a podpora** klikněte na **Aktivovat produkt** a do zobrazeného dialogového okna zadejte licenční klíč, který jste obdrželi při nákupu bezpečnostního produktu ESET.

Licenční klíč zadávejte přesně tak, jak je napsaný.

- Licenční klíč je unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.

Údaje z licenčního e-mailu doporučujeme zkopírovat (CTRL+C) a vložit do programu (CTRL+V). Při kopírování dejte pozor, abyste navíc nevložili mezeru.

Účet ESET HUB

ESET HUB je centrální brána k jednotné bezpečnostní platformě ESET PROTECT. Poskytuje centralizovanou správu identit, předplatného a uživatelů pro všechny moduly platformy ESET. ESET HUB umožňuje:

- Získat přehled o předplatném pro zabezpečení
- Kontrolovat využití a stav předplacených služeb
- Alokovat a spravovat granulární přístup k jednotlivým platformám ESET
- Jednotné přihlášení pro všechny připojené a dostupné platformy ESET

Tuto možnost můžete použít k aktivaci ESET Endpoint Security také pomocí starších nástrojů pro správu licencí: ESET Business Account nebo ESET MSP Administrator.

Můžete si vytvořit ESET HUB účet a přihlásit se pomocí své **e-mailové adresy** a **hesla**.

Pokud jste zapomněli heslo ke svému účtu, klikněte na **Zapomněl jsem heslo** a budete přesměrování na ESET HUB. Následně zadejte svoji e-mailovou adresu a potvrďte kliknutím na tlačítko **Odeslat**. Poté obdržíte e-mail s pokyny, jak obnovit heslo.

Jak použít klasické licenční údaje pro aktivaci produktu ESET pro ochranu koncových zařízení

Pokud máte uživatelské jméno a heslo, pro získání Licenčního klíče navštivte portál ESET Business Account. Na tomto portále si můžete stávající licenční údaje převést na licenční klíč.

Neúspěšná aktivace

Nejčastější problémy s aktivací ESET Endpoint Security mohou být:

- Licenční klíč je již používán.
- Zadali jste nesprávný licenční klíč.
- Informace v aktivačním formuláři chybí nebo jsou neplatné.
- Komunikace s aktivačním serverem se nezdařila.
- Žádné nebo blokované spojení s ESET aktivačními servery.

Ověřte, zda jste zadali správný licenční klíč nebo připojili licenci Offline, a zkuste aktivaci provést znovu.

Pokud se vám stále nedaří produkt aktivovat, náš průvodce vám poskytne odpovědi na nejčastější dotazy, aktivační chyby a problémy společně s informacemi týkajícími se licencování produktu (průvodce je dostupný v angličtině a vybraných jazycích).

- Spustit průvodce řešením potíží s aktivací produktu ESET

Registrace

Zaregistrujte svoji licenci vyplnění povinných polí a akci dokončete kliknutím na tlačítko **Pokračovat**. Pole označená jako povinná je nutné vyplnit. Tyto informace budou použity pouze pro záležitosti související s vaší ESET

licencí.

Průběh aktivace

ESET Endpoint Security se nyní aktivujte. Může chvíli trvat.

Úspěšná aktivace

Aktivace byla úspěšná a ESET Endpoint Security je nyní aktivován. ESET Endpoint Security si bude pravidelně stahovat aktualizace pro zajištění maximální úroveň ochrany počítače před škodlivým kódem. Pro pokračování klikněte na tlačítko **Dokončit**.

Známé problémy při instalaci

Pokud během instalace dojde k potížím, Průvodce instalací nabídne Poradce při potížích, který problém pokud možno vyřeší.

Pro spuštění klikněte na **Spustit Poradce při potížích**. Po dokončení postupujte podle doporučeného řešení.

Pokud problém přetrvává, podívejte se na seznam Známých chyb při instalaci a jejich řešení.

Začínáme

Tato kapitola poskytuje první seznámení s produktem ESET Endpoint Security a jeho základním nastavení.

Ikona v oznamovací oblasti

Nejdůležitější možnosti a funkce programu jsou dostupné přímo ze systémové oznamovací oblasti. Stačí kliknout pravým tlačítkem myši na ikonu programu .

> Kontextové menu ikony v oznamovací oblasti je dostupné pouze v případě, kdy je Režim spuštění grafického rozhraní nastaven na možnost Úplný.

Dočasně vypnout ochranu – zobrazí potvrzovací dialog, pomocí kterého vypnete detekční jádro, které chrání systém proti škodlivým útokům tím, že kontroluje soubory, e-maily a komunikaci prostřednictvím internetu. V rozbalovacím menu **časového intervalu** nastavte dobu, po kterou bude ochrana vypnuta.

Dočasně vypnout firewall – přepne firewall do neaktivního režimu. Pro více informací přejděte do kapitoly Síť.

Blokovat veškerou komunikaci – firewall zablokuje veškerou síťovou komunikaci. Pro obnovení komunikace klikněte na **Povolit veškerou komunikaci**.

Rozšířená nastavení – otevře Rozšířená nastavení ESET Endpoint Security. Pro otevření Rozšířených nastavení z hlavního okna programu stiskněte klávesu F5 nebo klikněte na **Nastavení** > **Rozšířená nastavení**.

Protokoly – protokoly obsahují informace o všech systémových událostech a poskytují přehled o nalezených

hrozbách.

Otevřít ESET Endpoint Security – kliknutím otevřete hlavní okno programu ESET Endpoint Security přímo z oznamovací oblasti.

Obnovit rozmístění oken – obnoví přednastavenou velikost a pozici okna ESET Endpoint Security na obrazovce.

Barevný režim – otevře rozšířené nastavení Uživatelského rozhraní, kde můžete změnit barvu grafického rozhraní.

Zkontrolovat aktualizace – spustí aktualizaci modulu nebo produktu. Tímto krokem získáte nejnovější aktualizace produktu. ESET Endpoint Security kontroluje aktualizace automaticky několikrát denně.

O programu – poskytuje informace o instalovaném programu ESET Endpoint Security a všech jeho programovaných modulech. Také zde naleznete informace o operačním systému a systémových prostředcích.

Klávesové zkratky

Pro rychlejší navigaci v produktu ESET Endpoint Security můžete použít také následující klávesové zkratky:

Klávesové zkratky	Akce
F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Šipka nahoru / šipka dolů	přesun v položkách rozbalovací nabídky
TAB	přesun na následující ovládací prvek v uživatelském rozhraní
Shift+TAB	přesun na předchozí ovládací prvek v uživatelském rozhraní
ESC	zavře zobrazené dialogové okno
Ctrl+U	zobrazí dialogové okno se základními informacemi pro technickou podporu ESET, kde mj. najdete identifikátor své licence a informace o počítači
Ctrl+R	obnoví pozici a velikost okna na výchozí hodnoty
ALT + šipka vlevo	přesun zpět
ALT + šipka vpravo	přesun vpřed
ALT+Home	přesun na úvodní obrazovku

Pro přesuny vpřed i zpět lze použít také tlačítka na myši.

Profily

Správa profilů se v ESET Endpoint Security používá na dvou místech – při **Volitelné kontrole** a **Aktualizaci**.

Kontrola počítače

K dispozici jsou čtyři předdefinované profily kontroly ESET Endpoint Security:

- **Smart kontrola počítače**: toto je výchozí profil pokročilé kontroly. Profil Smart kontrola počítače využívá technologii Smart optimalizace, pro vyloučení souborů, které byly při předchozí kontrole označeny jako čisté, a nedošlo u nich od té doby ke změně. Tím se zkracuje doba kontroly při současném minimálním

dopadu na zabezpečení systému.

- **Kontrola z kontextového menu**: Volitelnou kontrolu libovolného souboru můžete spustit z kontextového menu. Profil kontroly z kontextového menu umožňuje nastavit konfiguraci kontroly při jejím využití.
- **Hloubková kontrola počítače**: Profil hloubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.
- **Kontrola počítače**: Toto je výchozí profil používaný při standardní kontrole počítače.

Oblíbená nastavení kontroly počítače si můžete uložit do profilů pro jejich opakované použití v budoucnu. Doporučujeme vytvořit několik profilů s různými cíli a metodami kontroly, případně s dalšími parametry.

Pro vytvoření nového profilu otevřete Rozšířená nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** > **Seznam profilů** > **Změnit**. Kliknutím na **Změnit** na řádku **Seznam profilů** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. Chcete-li si vytvořit profil kontroly, který bude vyhovovat vašim potřebám, podívejte se do kapitoly ThreatSense, kde najdete popis jednotlivých parametrů pro nastavení kontroly.

> Chcete si vytvořit vlastní profil **kontroly počítače** a částečně vám vyhovuje nastavení předdefinovaného profilu, ale nechcete zároveň kontrolovat runtime packery nebo potenciálně nebezpečné aplikace a zároveň **Vždy vyřešit infekci**? V **Seznamu profilů** klikněte na tlačítko **Přidat** a profil pojmenujte. Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktualizační profil** nastavte si parametry kontroly podle potřeby, a změny uložte kliknutím na tlačítko OK.

Aktualizace

Editor profilů v Nastavení aktualizace umožňuje vytvářet nové aktualizační profily. Ty se používají pouze v případě, že používáte různé způsoby připojení na aktualizační servery.

Příkladem může být firemní notebook, který se v interní síti aktualizuje z mirroru, ale mimo firemní síť se aktualizace stahují ze serverů společnosti ESET. Po vytvoření profilů je ještě potřeba odpovídajícím způsobem upravit naplánované úlohy na záložce **Nástroje** > **Plánovač**. Jeden profil bude primární, druhý jako sekundární.

Aktualizační profil – aktuálně používaný profil. Pro jeho změnu vyberte jiný z rozbalovacího menu.

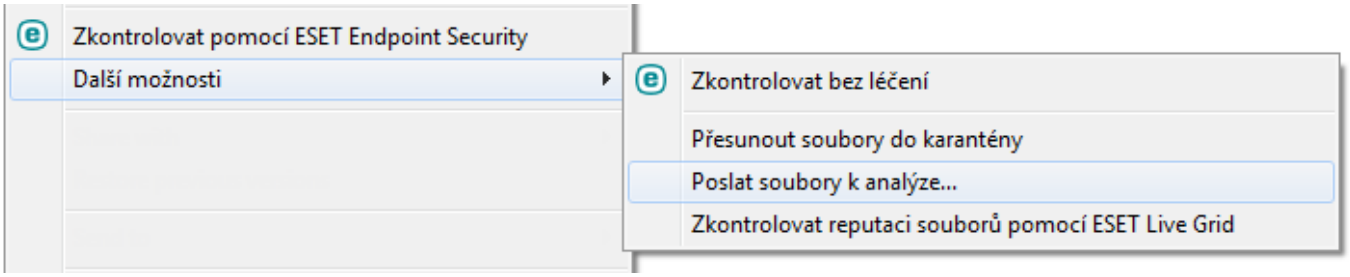
Seznam profilů – správa existujících aktualizačních profilů.

Kontextové menu

Kontextové menu se zobrazuje po kliknutí pravým tlačítkem myši na daný objekt. V tomto menu jsou následně dostupné akce, které je možné na daném objektu provést.

Do kontextového menu můžete integrovat také ovládací prvky produktu ESET Endpoint Security. Možnost nastavení této funkce je k dispozici v Rozšířených nastaveních > **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

Integrovat do kontextového menu – pomocí této možnosti integrujete ovládací prvky programu ESET Endpoint Security do kontextového menu.

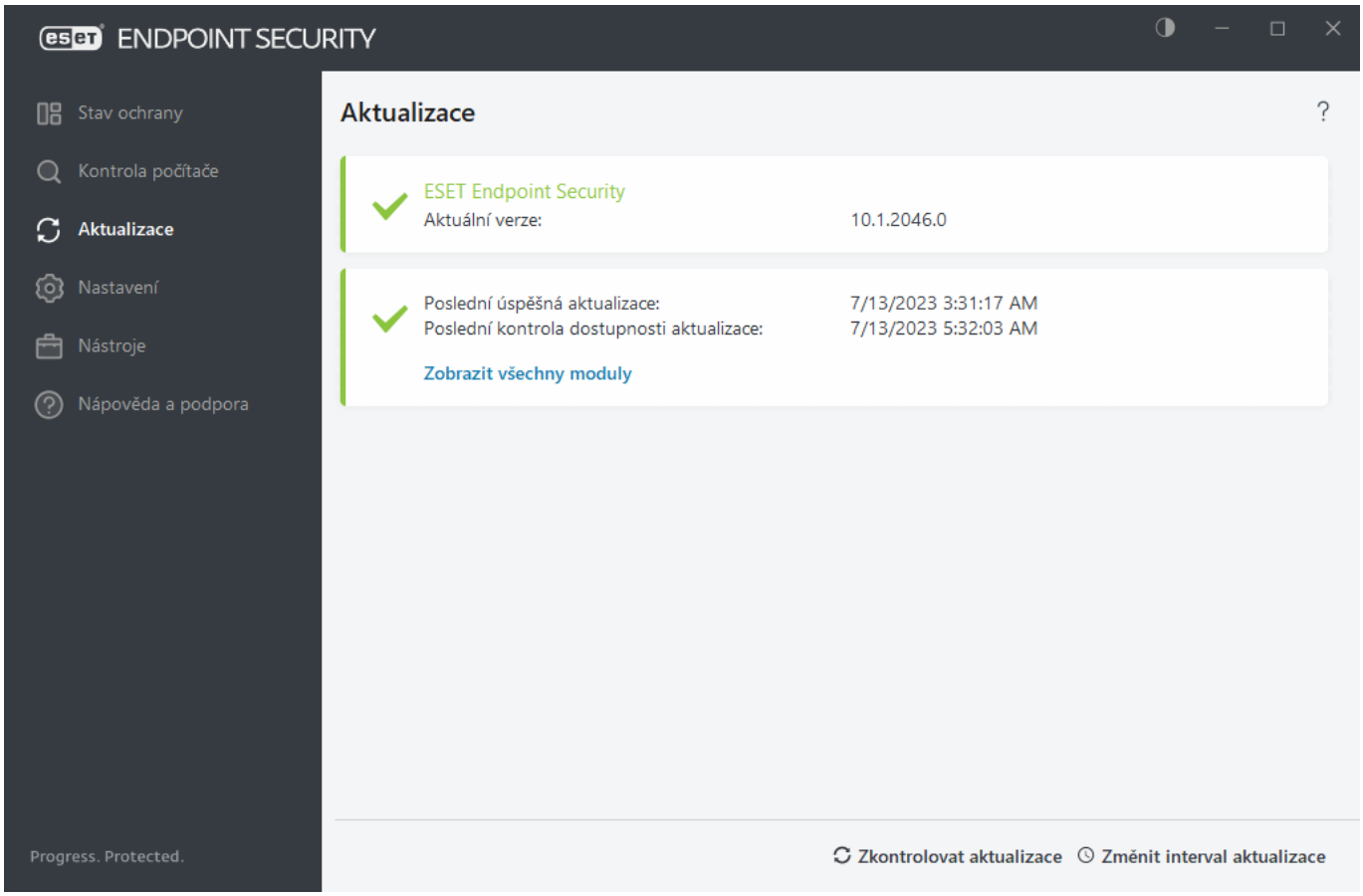


Nastavení aktualizace

Pravidelná aktualizace programu ESET Endpoint Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby program používal nejnovější detekční a programové moduly.

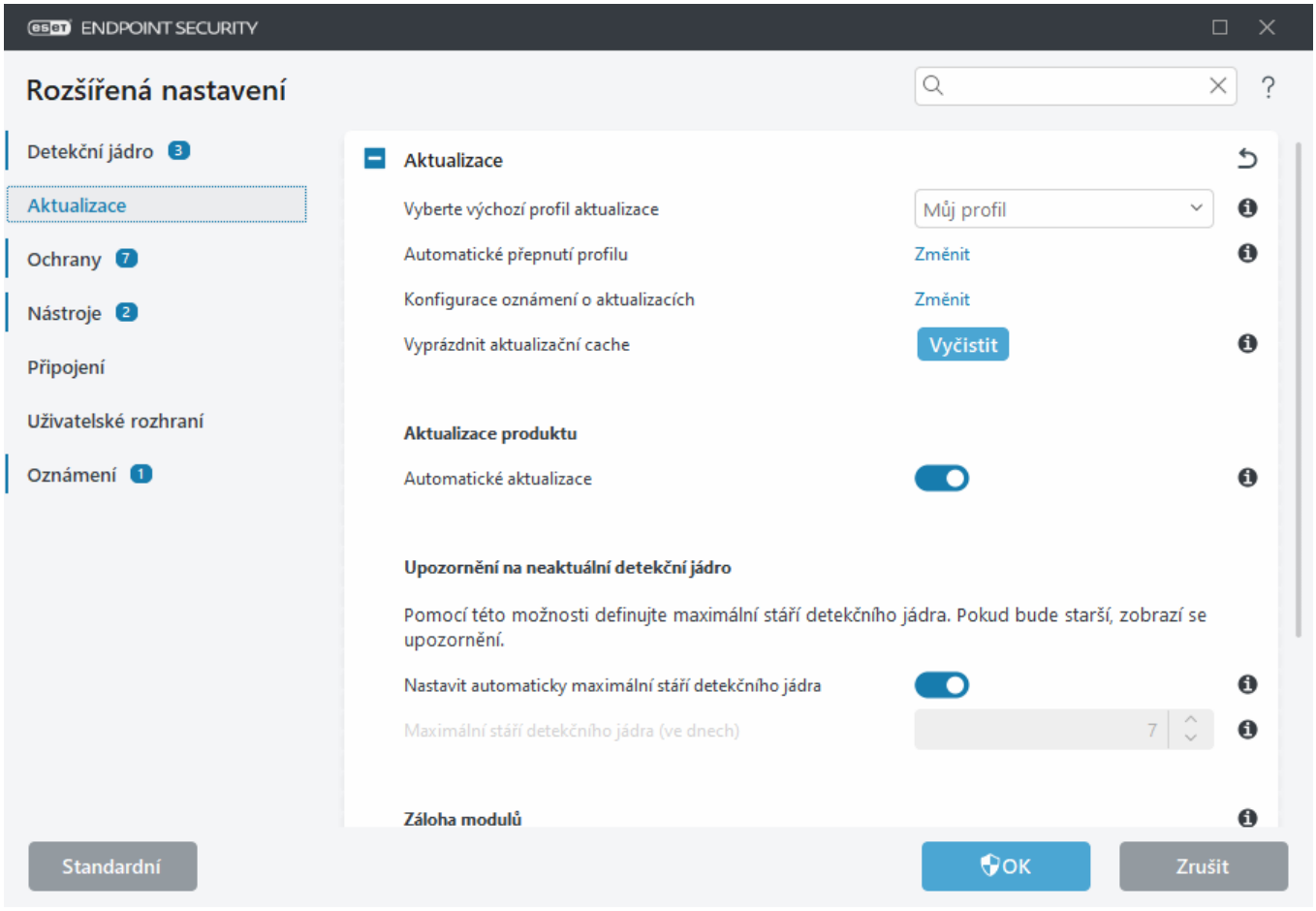
Informace o aktuálním stavu aktualizace jsou zobrazovány na záložce **Aktualizace** v hlavním okně programu. Naleznete zde informaci o datu a čase poslední úspěšné aktualizace, zda jsou moduly aktuální, případně jestli není potřeba program aktualizovat.

Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na tlačítko **Zkontrolovat aktualizace**.



V Rozšířeném nastavení > **Aktualizace** najdete další možnosti, například režim aktualizace, přístup k proxy serveru a připojení k síti LAN.

Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit**. Pokud po provedení této akce stále nebude možné moduly aktualizovat, přejděte do Databáze znalostí.

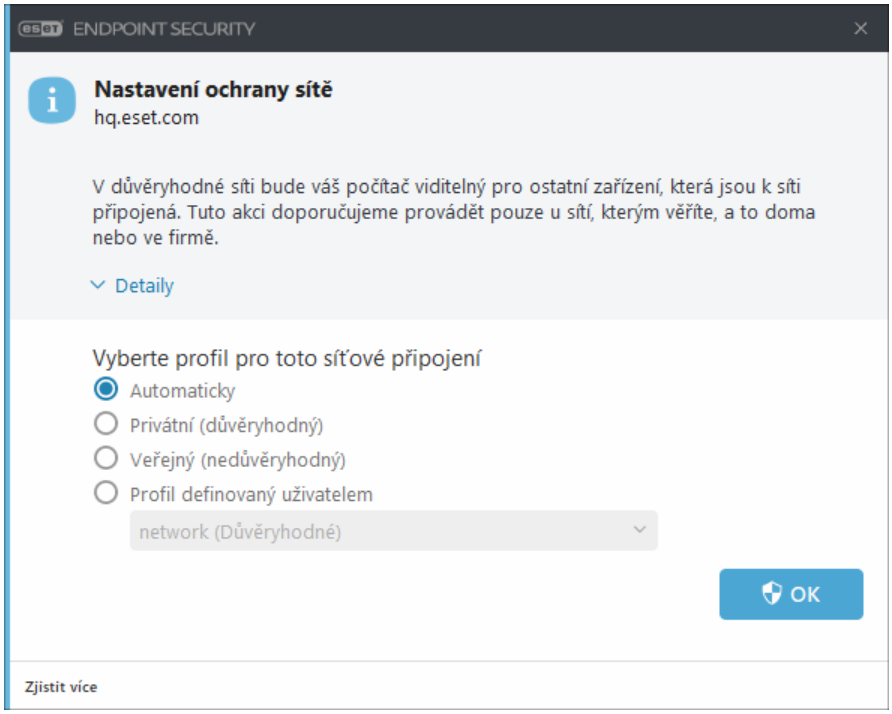


Ve výchozím nastavení je aktivní možnost **Automatický výběr serveru** v Rozšířených nastaveních > **Aktualizace** > **Profily** > **Aktualizace** > **Aktualizace modulů**. Tím je zajištěna aktualizace produktu ze serverů ESET. Toto nastavení doporučujeme ponechat tak, jak je.

Pro optimální běh programu je třeba, aby byl automaticky aktualizován. To je možné pouze v případě, že zadáte platný Licenční klíč na záložce **Nápověda a podpora** > **Aktivovat produkt**. Pokud nezadáte Licenční klíč po dokončení instalace, můžete jej zadat kdykoli poté. Více informací naleznete v kapitole Jak aktivovat ESET Endpoint Security?

Nastavení ochrany sítě

Ve výchozím nastavení převezme ESET Endpoint Security při detekci nového síťového připojení nastavení ze systému Windows. Chcete-li zobrazit dialogové okno při zjištění nové sítě, změňte Přiřazení profilu ochrany sítě na možnost **Zeptat se.** Konfigurace ochrany sítě se zobrazí vždy, když se počítač připojí k nové síti.



Můžete si vybrat z následujících profilů síťového připojení:

Automaticky – ESET Endpoint Security vybere profil automaticky na základě Spouštěčů nakonfigurovaných pro každý profil.

Privátní – pro důvěryhodné sítě (domácí nebo firemní síť). Vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti (přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít v bezpečných lokálních sítích. Tento profil je automaticky přiřazen síťovému připojení, pokud je nakonfigurováno jako doménová nebo privátní síť ve Windows.

Veřejná – pro nedůvěryhodné sítě (veřejná síť). Soubory a složky uložené ve vašem počítači nebudou pro ostatní uživatele v síti dostupné, stejně tak nebude počítač viditelný v síti. Sdílení systémových prostředků bude deaktivováno. Toto nastavení doporučujeme při připojení k bezdrátovým sítích. Tento profil je automaticky přiřazen každému síťovému připojení, které není nakonfigurováno jako doménová nebo privátní síť ve Windows.

Profil definovaný uživatelem – z rozbalovacího menu můžete vybrat profil, který jste vytvořili. Tato možnost je k dispozici pouze v případě, že jste vytvořili alespoň jeden vlastní profil.

⚠ Nesprávným nastavením sítě může být počítač ohrožen.

Filtrování obsahu webu

Pokud jste aktivovali Filtrování obsahu webu v ESET Endpoint Security, musíte také nastavit, pro které uživatelské účty bude filtrování aktivní. Další informace o tom, jak vytvořit specifická pravidla pro ochranu uživatelů před potenciálně nevhodným obsahem, naleznete v kapitoleFiltrování obsahu webu.

Blokované hashe

Používání ESET Inspect ve vašem prostředí umožňuje správcům blokovat přístup k zadaným spustitelným souborům na základě jejich hashe. Pokud správce zablokuje přístup ke spustitelnému souboru a vy se k němu pokusíte získat přístup, ESET Endpoint Security zobrazí toto oznámení:

Přístup k souboru byl zablokován – aplikace (zobrazí se název aplikace) se pokusila o přístup k souboru, který není povolen správcem.

Pokud jste správce a chcete povolit přístup k aplikaci uvedené v oznámení, přečtěte si kapitolu Blocked Hashes v ESET Inspect online nápovědě. Pokud jste uživatel a chcete změnit chování aplikace, obraťte se na správce.

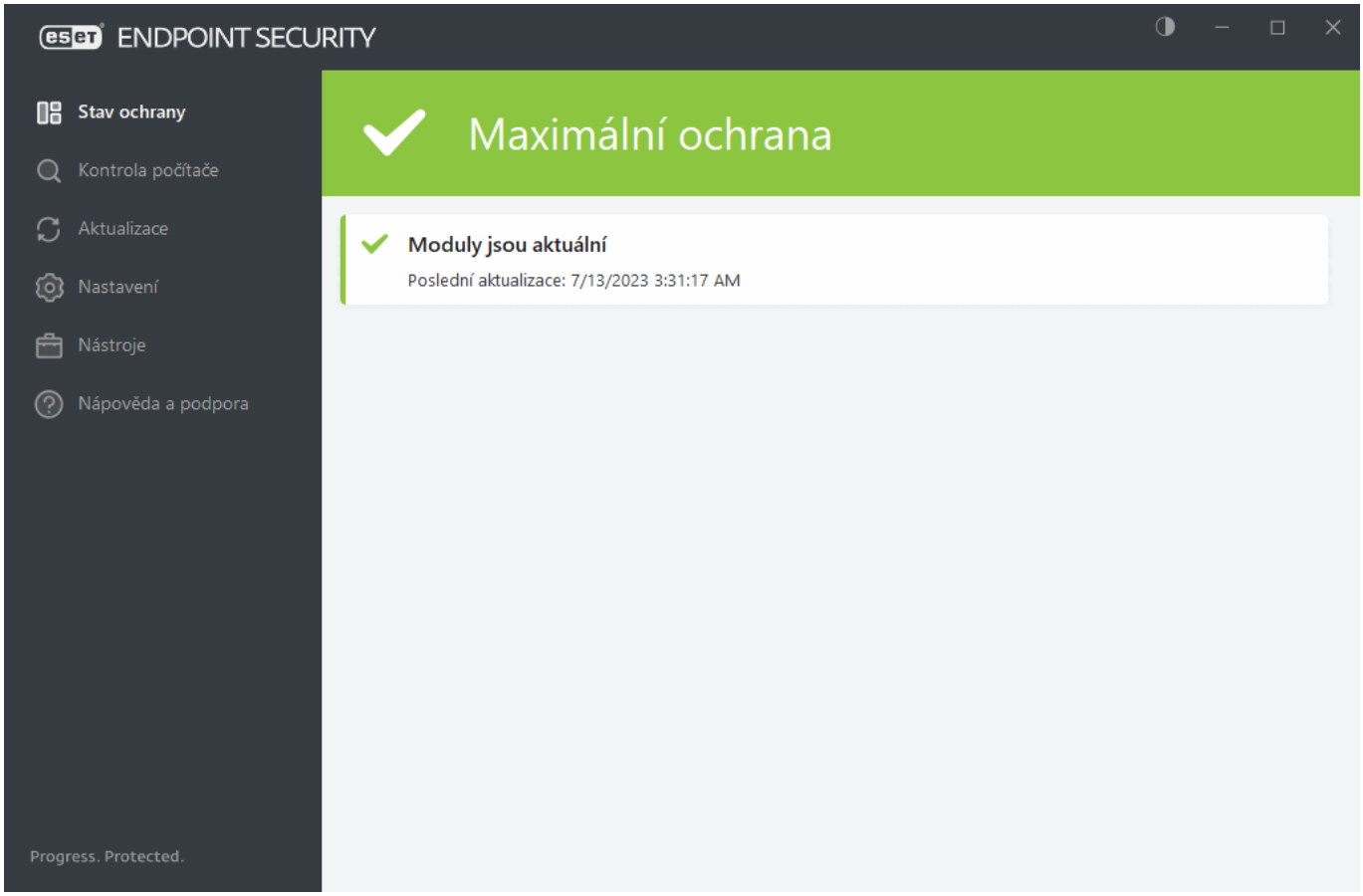
Práce s ESET Endpoint Security

Hlavní okno programu ESET Endpoint Security je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

> **Názorné ukázky**
> Názorné ukázky, jak otevřít hlavní okno produktu, máme k dispozici v Databázi znalostí v angličtině a několika dalších jazycích.

V pravém horním rohu hlavního okna programu si můžete navolit barevný režim, ve kterém se vám bude zobrazovat uživatelské rozhraní ESET Endpoint Security. Klikněte na ikonu pro **barevné schéma** (ikona se mění podle aktuálně vybraného barevného schématu) vedle ikony pro **minimalizaci** a z rozbalovacího menu vyberte barevný režim:

- **Stejný jako barva systému** – rozhraní ESET Endpoint Security se zobrazí ve stejném barevném schématu, jako uživatelské rozhraní vašeho operačního systému.
- **Tmavý** – ESET Endpoint Security bude zobrazen v tmavém režimu.
- **Světlý** – ESET Endpoint Security bude zobrazen ve světlém režimu.



Položky hlavního menu:

Stav ochrany – v přehledné formě poskytuje informace o stavu ochrany ESET Endpoint Security,

Kontrola počítače – v této části můžete spustit kontrolu svého počítače, definovat parametry vlastní kontroly, stejně tak provést kontrolu výměnných médií.

Aktualizace – zobrazuje informace o aktualizacích detekčního jádra a programových modulů.

Nástroje – poskytují přístup k funkcím, které zjednodušují správu programu a nabízejí další možnosti pro pokročilé uživatele.

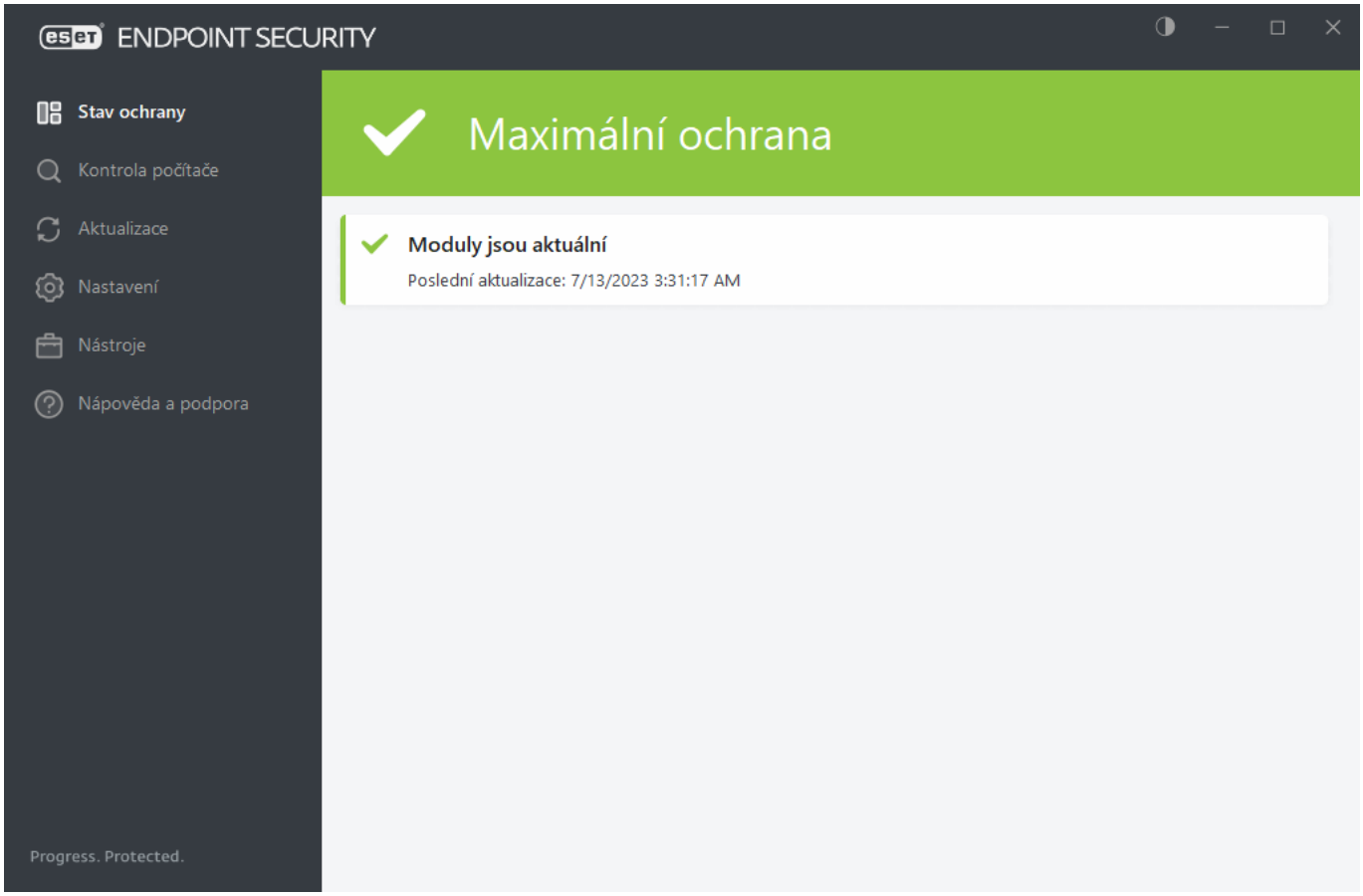
Nastavení - poskytuje možnosti konfigurovat funkce ochrany ESET Endpoint Security a přístup k Rozšířeným nastavením.

Nápověda a podpora – Zobrazuje informace o vaší licenci, nainstalovaném produktu ESET a odkazy na Online nápovědu, Databázi znalostí a Technickou podporu.

Stav ochrany

V okně **Stav ochrany** se zobrazují informace o aktuálním stavu ochrany zařízení a poslední aktualizaci. Zelená ikona a informace **Maximální ochrana** znamená, že je zajištěna maximální úroveň ochrany.

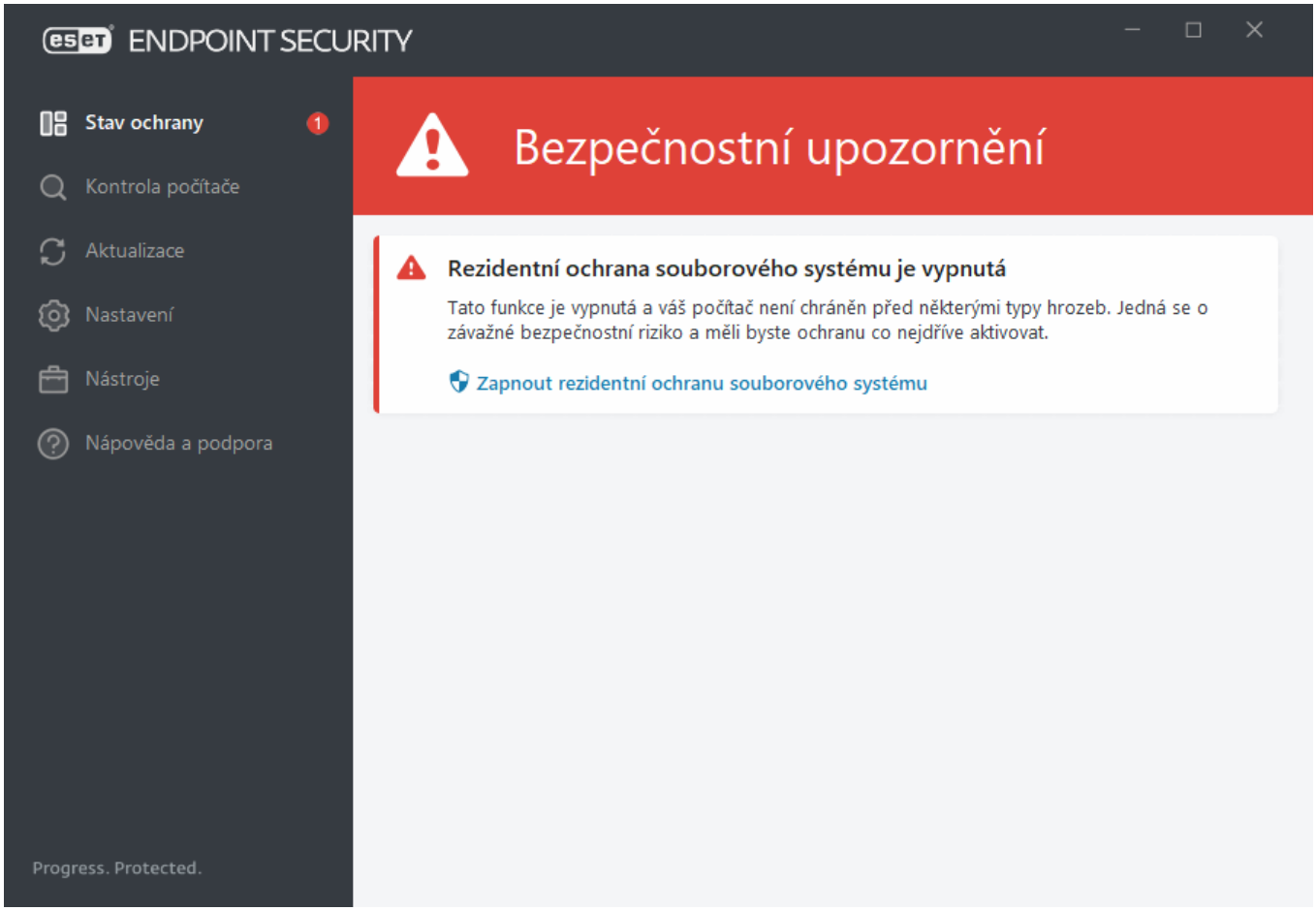
V okně **Stav ochrany** se zobrazují oznámení s podrobnými informacemi a doporučenými řešeními pro zlepšení zabezpečení ESET Endpoint Security, zapnutí dalších funkcí nebo zajištění maximální ochrany.



Zelená barva stavu ochrany a informace **Maximální ochrana** znamená, že je zajištěna maximální úroveň ochrany.

Co dělat, když program nepracuje správně?

Vedle plně funkčních programových modulů se zobrazí zelené zaškrtnutí. Pokud modul vyžaduje vaši pozornost, zobrazí se červený vykřičník nebo oranžová ikona oznámení. Další informace o modulu, včetně doporučení k obnovení plné funkčnosti se zobrazují v horní části okna. Chcete-li změnit stav modulu, klikněte v hlavním menu na položku **Nastavení** a poté klepněte na požadovaný modul.



Červená barva stavu ochrany, symbol "!" a informace "Není zajištěna maximální ochrana" signalizuje kritické problémy. Možné příčiny jsou:

- **Antivirová a antispywarová ochrana je dočasně vypnutá** – antivirovou a antispywarovou ochranu znovu aktivujete kliknutím na **Zapnout rezidentní ochranu** na záložce **Stav ochrany** nebo **Zapnout antivirovou a antispywarovou ochranu** na záložce **Nastavení**.
- Antivirová ochrana není funkční – nepodařilo se inicializovat virový skener. Většina součástí ESET Endpoint Security nebude funkční.
- **Anti-Phishingová ochrana není funkční** – tato funkce vyžaduje další moduly programu, které neběží.
- **Firewall je vypnutý** – v tomto případě ikona ochrany změní barvu na červenou a zobrazí se bezpečnostní upozornění vedle položky **Síť**. Znovu zapnout ochranu můžete kliknutím na **Zapnout filtrování**.
- **Inicializace firewallu se nezdařila** – firewall je vypnutý z důvodu problému s integrací do systému. Restartujte počítač co nejdříve.
- **Detekční jádro není aktuální** – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci detekčního jádra (dříve známého jako virová databáze). V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Mezi nejčastější důvody patří nesprávně zadaná ověřovací data nebo nesprávně nastavené připojení k internetu.
- **Produkt není aktivován** nebo **Vaše licence vypršela** – ikona stavu ochrany změní barvu na červenou. Program nebude možné od této chvíle aktualizovat. Přečtěte si v okně s upozorněním, jak licenci prodloužit.
- **Host Intrusion Prevention System (HIPS) je vypnutý** – toto hlášení upozorňuje na to, že HIPS je vypnutý. Váš počítač není chráněn proti některým hrozbám a ochranu byste měli co nejdříve aktivovat kliknutím na možnost **Zapnout HIPS**.
- **Není naplánována pravidelná aktualizace** – ESET Endpoint Security nebude automaticky kontrolovat dostupnost aktualizací.

- **Přístup k síti byl zablokován** – toto upozornění se zobrazí v případě, kdy byl počítač **Izolován od sítě** prostřednictvím klientské úlohy zaslané z ESET PROTECT. Pro více informací kontaktujte správce vašeho systému.
- **Rezidentní ochrana souborového systému je dočasně pozastavená** – rezidentní ochrana byla vypnuta uživatelem a počítač není chráněn před hrozbami. Váš počítač není chráněn před hrozbami. Pro opětovné zapnutí Rezidentní ochrany souborového systému klikněte na Zapnout rezidentní ochranu.


Žlutá barva stavu ochrany, symbol "i" a informace, že je vyžadována vaše pozornost, nepředstavuje kritický problém. Možné příčiny jsou:

- **Ochrana přístupu na web je vypnutá** – znovu zapnout ji můžete kliknutím na bezpečnostní upozornění a možnost **Zapnout Ochranu přístupu na web**.
- **Blíží se konec platnosti licence** / **Platnost vaší licence dnes vyprší** – ikona stavu ochrany se zobrazí s vykřičníkem. Poté, co licence vyprší, se program přestane aktualizovat a ikona stavu ochrany změní barvu na červenou.
- **Ochrana proti zapojení do botnetu je dočasně vypnutá** – pro vyřešení klikněte na možnost **Zapnout ochranu proti zapojení do botnetu**.
- **Ochrana proti síťovým útokům (IDS) je dočasně vypnutá** –kliknutím na **Zapnout ochranu proti síťovým útokům (IDS)** tuto funkci znovu povolíte.
- **Antispamová ochrana poštovních klientů je dočasně vypnutá** – kliknutím na **Povolit Antispamovou ochranu poštovních klientů** tuto funkci znovu povolíte.
- **Filtrování obsahu webu je dočasně vypnuté** – pro vyřešení klikněte na možnost **Zapnout filtrování obsahu webu**.
- **Dočasná změna nastavení je aktivní** – je možné dočasně konfigurovat nastavení, které je jinak striktně vynucené politikou. Pouze oprávněný uživatel může dočasná měnit nastavení. Pro více informací přejděte do kapitoly Jak použít režim dočasné změny nastavení.
- **Správa zařízení je dočasně vypnutá** – pro vyřešení klikněte na možnost **Zapnout Správu zařízení**.

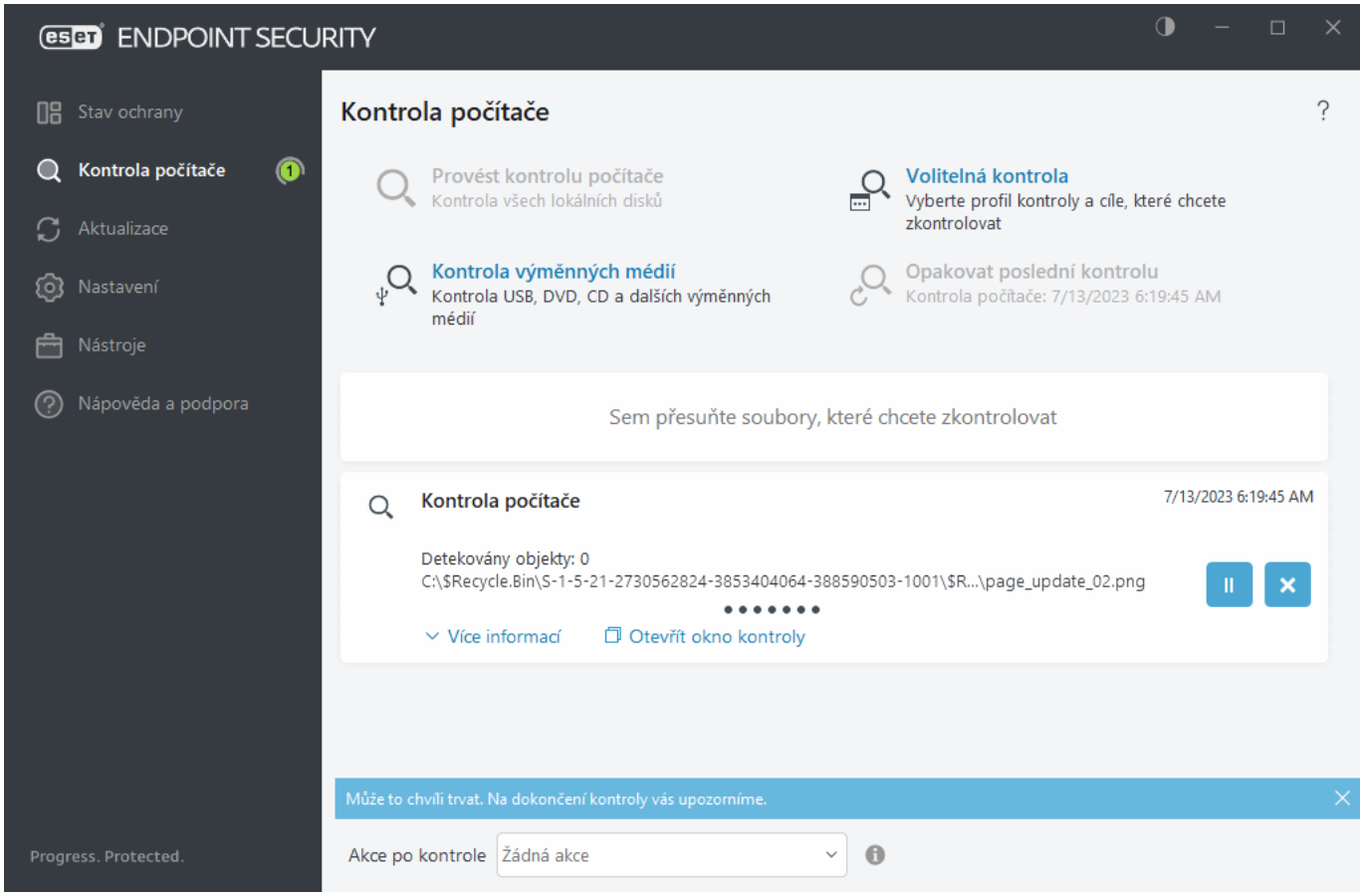
Pro potlačení stavů zobrazovaných na úvodní záložce produktu ESET Endpoint Security přejděte do kapitoly Stavy aplikace.

Pokud uvedený návrh na řešení problému nezabral, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zobrazte nápovědu nebo přejděte do ESET Databáze znalostí. Pokud i přesto budete potřebovat pomoc, můžete odeslat dotaz na technickou podporu. Specialisté technické podpory ESET vám odpoví v co nejkratším možném čase a pomohou vám s řešením problému.

Pokud máte na produkt aplikovanou politiku (například z ESET PROTECT), v závislosti na nastavení definované v politice nemusí být odkaz na aktivaci funkce/vyřešení problému funkční (bude zašedlý).

Kontrola počítače

Důležitou součástí antivirového ESET Endpoint Security je volitelná kontrola. Díky ní si spustíte vlastní kontrolu jednotlivých složek a souborů v počítači. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infikované soubory, ale v rámci prevence i průběžně. Hloubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech, aby byly detekovány případné viry, které v době zápisu na disk nebyly zachyceny Rezidentní ochranou souborového systému. Taková situace může nastat, pokud byla rezidentní ochrana v té době vypnutá nebo program neměl aktuální detekční moduly, případně soubor v době zápisu na disk program nebyl vyhodnocen jako virus.



K dispozici jsou dva typy **kontroly počítače**. Pokud kliknete na možnost **Provést kontrolu počítače**, spustí se rychlá kontrola systému a předdefinovaným nastavení. V případě, že si chcete upravit parametry kontroly, použijte možnost **Volitelná kontrola**, v rámci níž si můžete definovat profil i cíle kontroly.

Více informací o procesu kontroly naleznete v kapitole Průběh kontroly.

Provést kontrolu počítače

Tato možnost slouží pro rychlé spuštění kontroly počítače a automaticky léčí nebo odstraňuje infikované soubory a nevyžaduje interakci uživatele. Výhodou této kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. Zkontrolují se všechny soubory na lokálních discích a nalezené hrozby jsou automaticky vyléčeny nebo odstraněny. Úroveň léčení je nastavena na standardní úroveň. Více informací o úrovních léčení si přečtěte v kapitole Úroveň léčení.

Pro zkontrolování konkrétního souboru nebo složky ji můžete přetáhnout (**Drag and drop**) do zvýrazněné oblasti. Po přesunutí souboru se okno aplikace přesune do popředí.

V kontextovém menu tlačítka **Pokročilé kontroly** jsou dostupné následující možnosti kontroly počítače:

Volitelná kontrola

Volitelné kontrola umožňuje zadat parametry kontroly, například cíle a metody kontroly. Výhodou **volitelné kontroly** je možnost podrobně specifikovat její parametry. Nastavenou konfiguraci můžete uložit do uživatelských profilů využitelných při opakované kontrole za použití stejných parametrů.

Kontrola výměnných médií

Podobně jako možnost **Provést kontrolu počítače** – spustí rychlou kontrolu výměnných médií (CD/DVD/USB), které jsou aktuálně připojené/vložené do počítače. To je užitečné ve chvíli, když připojíte USB zařízení k počítači a potřebujete zjistit, zda neobsahuje škodlivý kód a další potenciální hrozby.

Tuto kontrolu můžete také spustit tak, že při definování **Volitelné kontroly** kliknete na ozubené kolečko, v rozbalovacím menu **Cíle kontroly** vyberete možnost **Výměnná média** a kliknete na tlačítko **Zkontrolovat**.

Opakovat poslední kontrolu

Pomocí této možnosti spustíte naposledy prováděnou kontrolu se stejnými cíli i parametry.

Rozbalovací menu **Akce po kontrole** umožňuje vybrat akci, která se má provést po dokončení kontroly:

- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.
- **Vypnout** – počítač se po dokončení kontroly vypne,
- **Restartovat v případě potřeby** – počítač se po dokončení kontroly restartuje, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Restartovat** – počítač se po dokončení kontroly restartuje.
- **V případě potřeby vynutit restart** – po dokončení kontroly se vynutí restartování počítače, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Vynutit restart** – po dokončení kontroly dojde k automatickému zavření všech otevřených aplikací a počítač se restartuje.
- **Režim spánku** – aktuální relace se uloží do operační paměti a počítač přejde do úsporného stavu. Následné probuzení počítače je rychlé a můžete ihned pokračovat v rozdělené činnosti.
- **Hibernovat** – uloží aktuální relaci na pevný disk a počítač se kompletně vypne. Při další spuštění počítače se obnoví poslední stav.

> Akce **Režim spánku** nebo **Hibernace** je dostupná na základě Nastavení napájení a režimu spánku, případně možnostech vašeho zařízení. Mějte na paměti, že uspaný počítač je pouze v režimu spánku a stále běží. Stále je napájen ze sítě, případně z baterie. Pro maximální výdrž baterie doporučujeme vybrat možnost Hibernovat.

Vybraná akce se provede po dokončení všech běžících kontrol. Pokud je vybrána možnost **Vypnout** nebo **Restartovat**, zobrazí se potvrzovací dialogové okno s 30sekundovým odpočtem (kliknutím na tlačítko **Zrušit vypnutí/restartování** akci přerušíte).

> Doporučujeme provádět kontrolu počítače alespoň jednou měsíčně. Pro pravidelnou kontrolu počítače můžete využít naplánované úlohy, jejichž konfiguraci naleznete v sekci **Nástroje** > **Plánovač**. Jak naplánovat týdenní kontrolu počítače?

Spuštění volitelné kontroly

Pokud chcete zkontrolovat například jen konkrétní disk, vybranou složku atp., můžete k tomu použít volitelnou složku. Spustíte ji tak, že v hlavním menu programu přejdete na záložku **Kontrola počítače** a klikněte na možnosti **Pokročilé kontroly** > Volitelná kontrola. Následně ze stromové struktury vyberte cíle, které chcete zkontrolovat na přítomnost hrozeb.

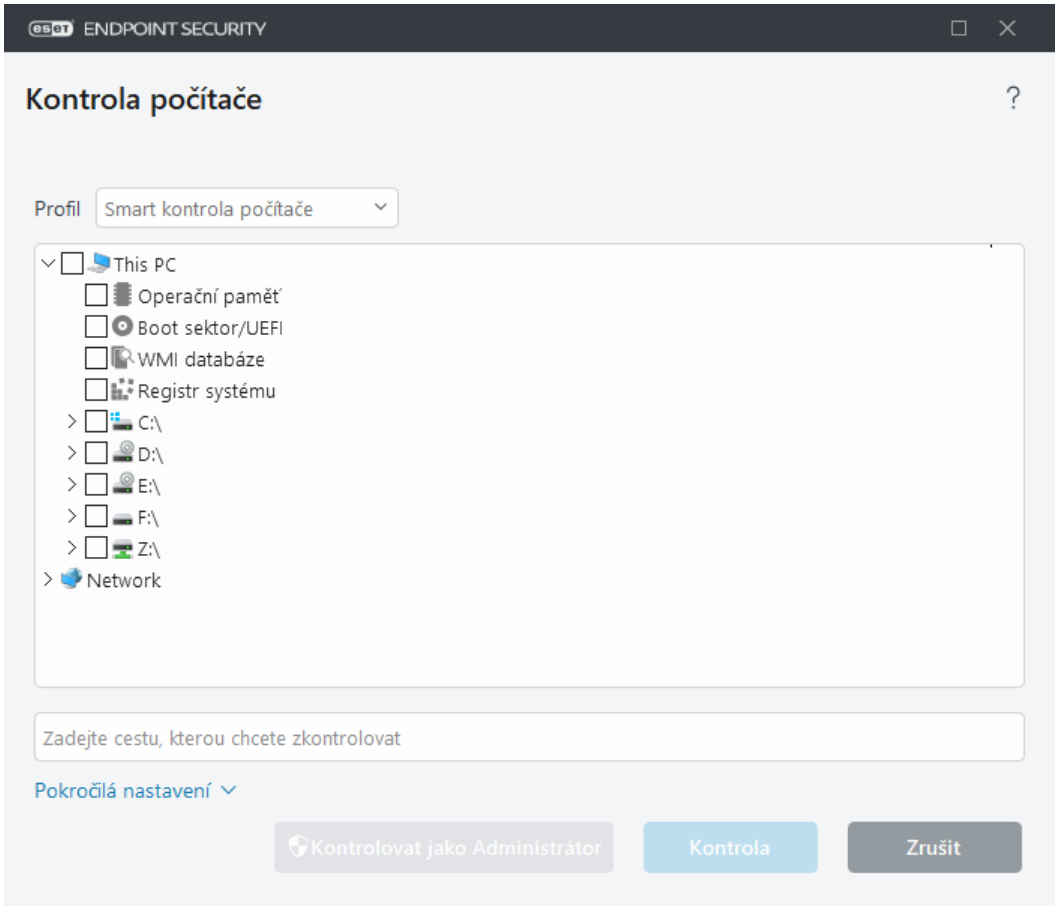
Pomocí rozbalovacího menu **Profil** si můžete vybrat jeden z předdefinovaných profilů kontroly. Výchozím profilem je **Smart kontrola počítače**. Dále jsou dostupné tři předdefinované profily pojmenované **Hloubková kontrola počítače**, **Kontrola z kontextového menu** a **Kontrola počítače**. Navzájem se liší odlišným nastavením parametrů skenovacího jádra ThreatSense. Dostupné možnosti jsou popsány v Rozšířených nastaveních > **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** > ThreatSense.

Další cíle kontroly si můžete vybrat ve stromové struktuře.

- **Operační paměť** – kontrola všech procesů a dat aktuálně nahraných v operační paměti.
- **Boot sektory/UEFI** – kontrola přítomnosti škodlivého kódu v boot sektorech disků a UEFI. Pro více informací o UEFI skeneru přejděte do slovníku pojmů.
- **WMI databáze** – kontrola celé Windows Management Instrumentation (WMI) databáze, všech jmenných prostorů, tříd instancí a vlastností. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor.
- **Registr systému** – kontrola celého registru systému, všech klíčů a podklíčů. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor. Při léčení detekce zůstane v registru odkaz, aby se zabránilo ztrátě důležitých dat.

Pro rychlý přesun k požadovanému cíli kontroly (souboru nebo složce), zadejte jeho cestu do textového pole zobrazeném pod stromovou strukturou. Mějte na paměti, že se v cestě rozlišuje velikost písmen. Použitím zaškrtávacího pole ve stromové struktuře přidáte daný cíl do seznamu cílů, které se mají kontrolovat.

> **Jak naplánovat každý týden kontrolu počítače?**
> Přečtěte si kapitolu Jak naplánovat kontrolu počítače jednou za týden?.



Parametry léčení použité v daném profilu kontroly můžete změnit v Rozšířených nastaveních > **Detekční jádro** >

Detekce škodlivého kódu > **Volitelná kontrola** > **ThreatSense** > **Léčení**. V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, klikněte na **Rozšířená nastavení** a následně vyberte možnost **Neléčit**. Historie kontrol je zaznamenána do protokolu kontrol.

Vybráním možnosti **Ignorovat výjimky** nebudou brány v potaz výjimky a dané soubory se zkontrolují.

Kliknutím na tlačítko **Kontrolovat** spustíte kontrolu počítače s nastavenými parametry.

Kliknutím na tlačítko **Kontrolovat jako Administrátor** spustíte kontrolu po účtem Administrátora. Tuto funkci použijte v případě, že aktuálně přihlášený uživatel nemá dostatečná práva pro kontrolu složek. Mějte na paměti, že tlačítko není dostupné, pokud uživatel nemůže provádět UAC operace jako administrátor.

Protokol kontroly po jejím ukončení zobrazíte kliknutím na tlačítko Zobrazit protokol.

Průběh kontroly

Okno průběhu kontroly zobrazuje aktuální stav kontroly a počet souborů, které obsahují škodlivý kód.

Je normální, že některé soubory, například soubory chráněné heslem nebo soubory používané výhradně systémem (například *pagefile.sys* a některé soubory protokolů), nelze kontrolovat. Další podrobnosti najdete v článku v Databázi znalostí.

Jak naplánovat každý týden kontrolu počítače?
Přečtěte si kapitolu Jak naplánovat kontrolu počítače jednou za týden?.

Průběh kontroly – ukazatel průběhu zobrazuje stav probíhající kontroly.

Cíl – název právě kontrolovaného souboru a jeho umístění.

Detekovány objekty – zobrazuje celkový počet kontrolovaných souborů, nalezených hrozeb a hrozeb vyčištěných během kontroly.

Kliknutím na Více informací se zobrazí následující informace:

- **Uživatel** – jméno uživatelského účtu, který spustil kontrolu.
- **Zkontrolováno objektů** – počet již zkontrolovaných objektů.
- **Doba zobrazení** – uplynulý čas.

Ikona pozastavení – přeruší kontrolu.

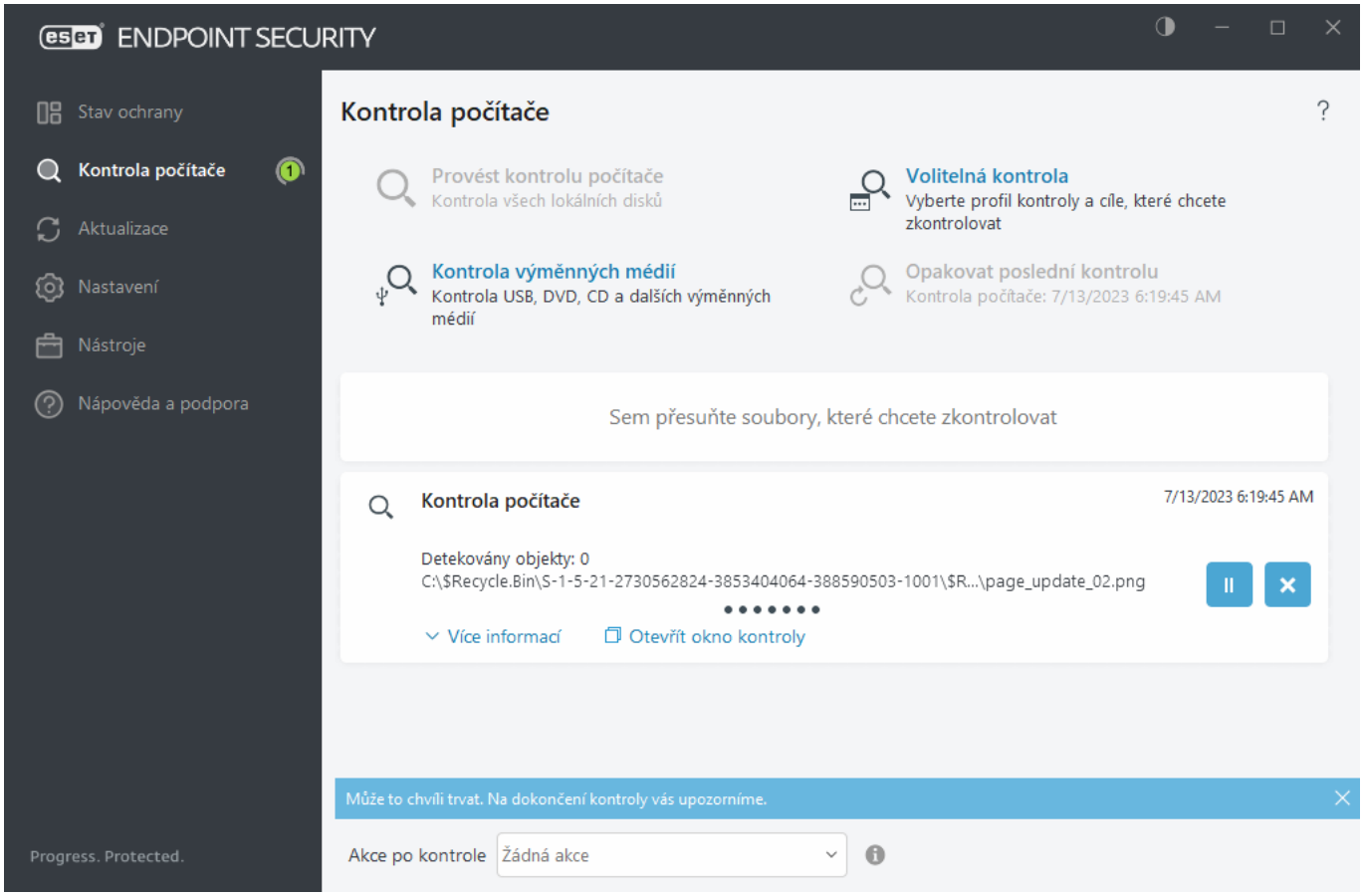
Pokračovat – možnost se zobrazí po pozastavení kontroly. Po kliknutí na ikonu se pokračujte v kontrole.

Ikona Stop – ukončí kontrolu.

Klepnutím na **Otevřít okno kontroly** otevřete Protokol kontroly počítače s podrobnějšími informacemi o kontrole.

Rolovat výpis protokolu kontroly – pokud je tato možnost zapnuta, v dialogovém okně protokolu kontroly uvidíte vždy naposledy zkontrolované soubory.

Pro zobrazení detailních informací o aktuálně probíhající kontrole klikněte na možnost **Více informací** nebo na **Otevřít okno kontroly**. Další paralelní kontrolu spustíte kliknutím na **Provést kontrolu počítače** nebo **Pokročilé kontroly** > **Volitelná kontrola**.



Rozbalovací menu **Akce po kontrole** umožňuje vybrat akci, která se má provést po dokončení kontroly:

- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.
- **Vypnout** – počítač se po dokončení kontroly vypne,
- **Restartovat v případě potřeby** – počítač se po dokončení kontroly restartuje, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Restartovat** – počítač se po dokončení kontroly restartuje.
- **V případě potřeby vynutit restart** – po dokončení kontroly se vynutí restartování počítače, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Vynutit restart** – po dokončení kontroly dojde k automatickému zavření všech otevřených aplikací a počítač se restartuje.
- **Režim spánku** – aktuální relace se uloží do operační paměti a počítač přejde do úsporného stavu. Následné probuzení počítače je rychlé a můžete ihned pokračovat v rozdělené činnosti.
- **Hibernovat** – uloží aktuální relaci na pevný disk a počítač se kompletně vypne. Při další spuštění počítače se obnoví poslední stav.

Akce **Režim spánku** nebo **Hibernace** je dostupná na základě Nastavení napájení a režimu spánku, případně možnostech vašeho zařízení. Mějte na paměti, že uspaný počítač je pouze v režimu spánku a stále běží. Stále je napájen ze sítě, případně z baterie. Pro maximální výdrž baterie doporučujeme vybrat možnost Hibernovat.

Vybraná akce se provede po dokončení všech běžících kontrol. Pokud je vybrána možnost **Vypnout** nebo **Restartovat**, zobrazí se potvrzovací dialogové okno s 30sekundovým odpočtem (kliknutím na tlačítko **Zrušit**

vypnutí/restartování akci přerušíte).

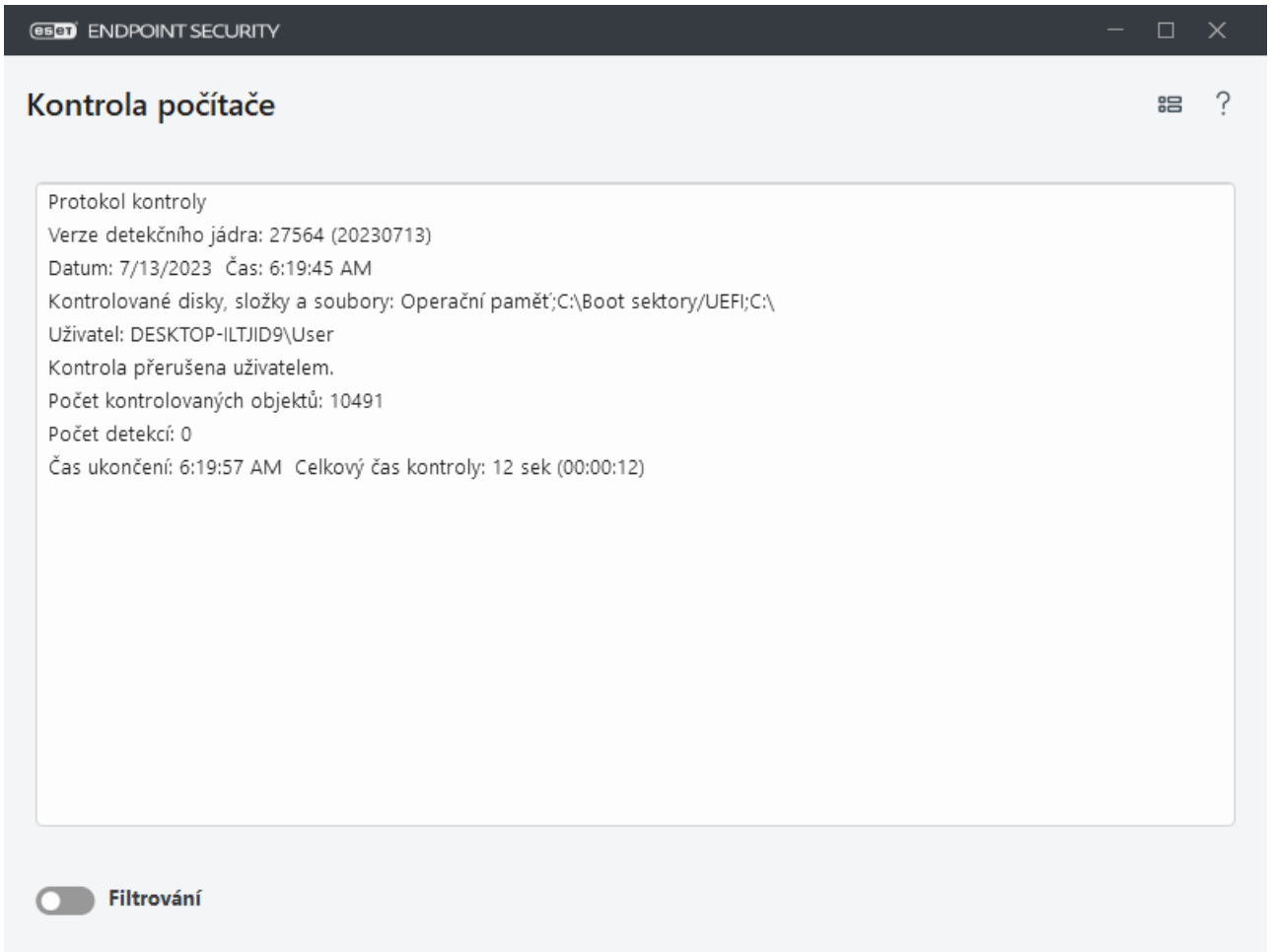
Protokol kontroly počítače

Podrobné informace týkající se konkrétní kontroly můžete zobrazit v Protokolech. Protokol kontroly obsahuje následující informace:

- Verze použitého detekčního jádra
- Datum a čas zahájení
- Kontrolované disky, složky a soubory
- Název volitelné kontroly (pouze u plánované kontroly)
- Uživatel, který spustil kontrolu.
- Stav kontroly
- Počet zkontrolovaných objektů
- Počet nalezených detekcí
- Čas dokončení
- Doba kontroly

> Nové spuštění volitelné kontroly počítače je přeskočeno, pokud stejná naplánovaná úloha stále běží. Přeskočená naplánovaná kontrola vytvoří Protokol kontroly s 0 kontrolovaných objektů a stavem **Kontrola se nespustila, protože stále probíhá předchozí kontrola**.

Pro zobrazení starších protokolů kontrol klikněte v hlavním okně programu na záložku **Nástroje** > **Protokoly**. V rozbalovacím menu vyberte možnost **Kontrola počítače** a poklepejte na požadovaný záznam.



Více informací týkajících se výskytu záznamů "Nelze otevřít", "chyba při otevírání" a/nebo "poškozený archiv" poškozené" v protokolech kontroly naleznete v naší Databázi znalostí.

Kliknutím na přepínací ikonu **Filtrování** otevřete okno Filtrování protokolu, kde můžete definovat vlastní kritéria pro zúžení vyhledávání. V kontextovém menu jednotlivých záznamů protokolu naleznete následující možnosti:

Akce	Použití
Filtrovat stejné záznamy	Aktivuje filtrování protokolu. V protokolu se následně zobrazí pouze záznamy stejného typu, odpovídající aktuálně vybranému záznamu.
Filtr	Tato možnost otevře okno Filtrování protokolu a umožňuje definovat kritéria pro konkrétní položky protokolu. Klávesová zkratka: `Ctrl+Shift+F`
Zapnout filtr	Zde se aktivuje nastavení filtru. Pokud aktivujete filtr poprvé, je třeba definovat nastavení a otevře se okno Filtrování protokolu.
Zrušit filtr	Vypne filtr (stejně jako kliknutím na přepínač v dolní části).
Kopírovat	Zkopíruje zvýrazněné záznamy do schránky. Klávesová zkratka: `Ctrl+C`
Kopírovat vše	Zkopíruje všechny záznamy v okně.
Export	Exportuje zvýrazněné záznamy do schránky do XML souboru.
Exportovat vše…	Pomocí této možnosti zkopírujete všechny záznamy v okně do XML souboru.
Popis detekce…	Po kliknutí budete přesměrování do ESET Encyklopedie hrozeb, kde naleznete informace o jednotlivých hrozbách.

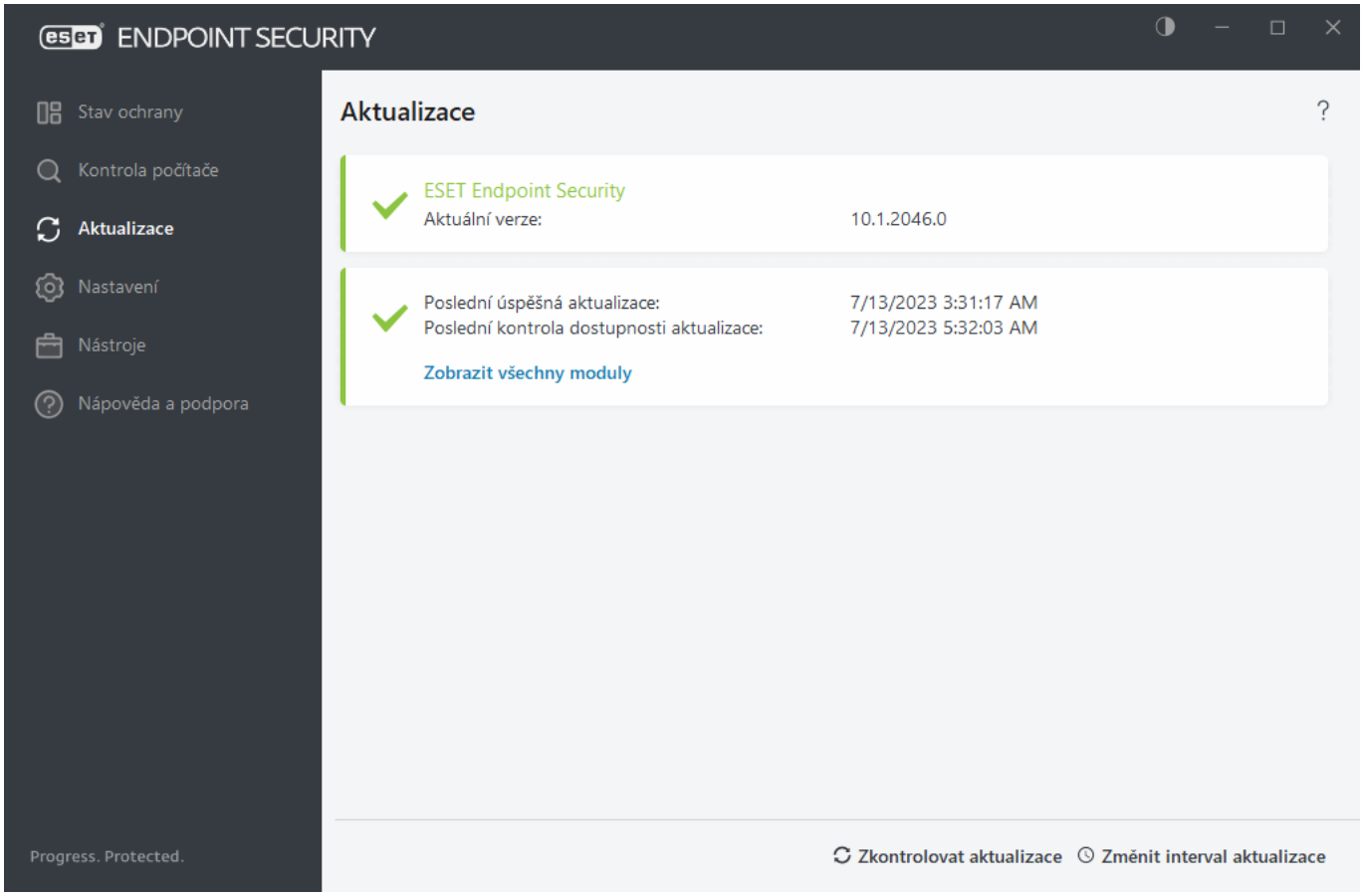
Aktualizace

Pravidelná aktualizace programu ESET Endpoint Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby program používal nejnovější detekční a programové moduly.

Informace o aktuálním stavu aktualizace jsou zobrazovány na záložce **Aktualizace** v hlavním okně programu. Naleznete zde informaci o datu a čase poslední úspěšné aktualizace, zda jsou moduly aktuální, případně jestli není potřeba program aktualizovat.

Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na tlačítko **Zkontrolovat aktualizace**. Pravidelná aktualizace modulů a komponent je důležitým aspektem pro zachování plné ochrany před škodlivým kódem. Věnujte prosím pozornost konfiguraci a práci modulů. Pro příjem automatických aktualizací je třeba produkt aktivovat pomocí licenčního klíče. Pokud jste tak neučinili během instalace, je nutné aktivovat ESET Endpoint Security, aby bylo možné přistupovat k aktualizačním serverům společnosti ESET. Licenční klíč jste obdrželi po nákupu nebo registraci ESET Endpoint Security.

Pokud jste ESET Endpoint Security aktivovali offline licenčním souborem, ve kterém není obsaženo uživatelské jméno a heslo, při pokusu o aktualizaci ze serverů ESET se zobrazí chyba **Moduly se nepodařilo aktualizovat**. Mějte na paměti, že v tomto případě můžete stahovat aktualizovat pouze z mirroru.



Aktuální verze – zobrazuje číslo verze produktu ESET Endpoint Security, který máte nainstalován.

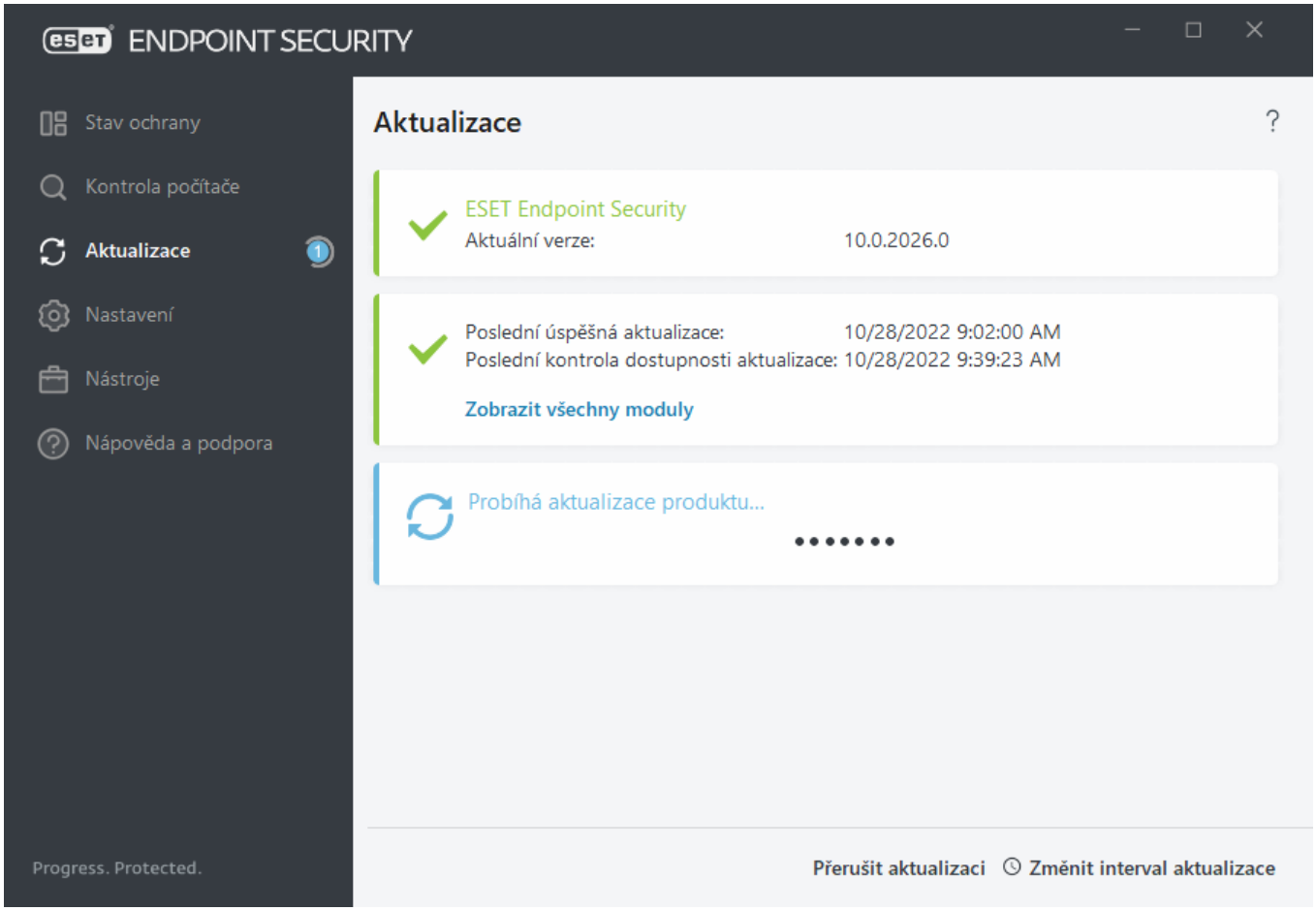
Poslední úspěšná aktualizace – zobrazuje datum, kdy se program naposledy úspěšně aktualizoval. Ujistěte se, že je datum není příliš staré, což znamená, že detekční jádro je aktuální.

Poslední kontrola dostupnosti aktualizace – zobrazuje datum, kdy se program naposledy úspěšně připojil k aktualizačním serverům a ověřil, zda není dostupná nová verze modulů.

Zobrazit všechny moduly – kliknutím si zobrazíte seznam používaných programových modulů.

Průběh stahování

V případě, že jsou na aktualizačních serverech dostupné nové moduly, po kliknutí na tlačítko **Zkontrolovat aktualizace** se spustí proces stahování. Zároveň se zobrazí průběh stahování souboru aktualizace a zbývající čas do konce. Kliknutím na tlačítko **Přerušit aktualizaci** aktualizaci zastavíte.



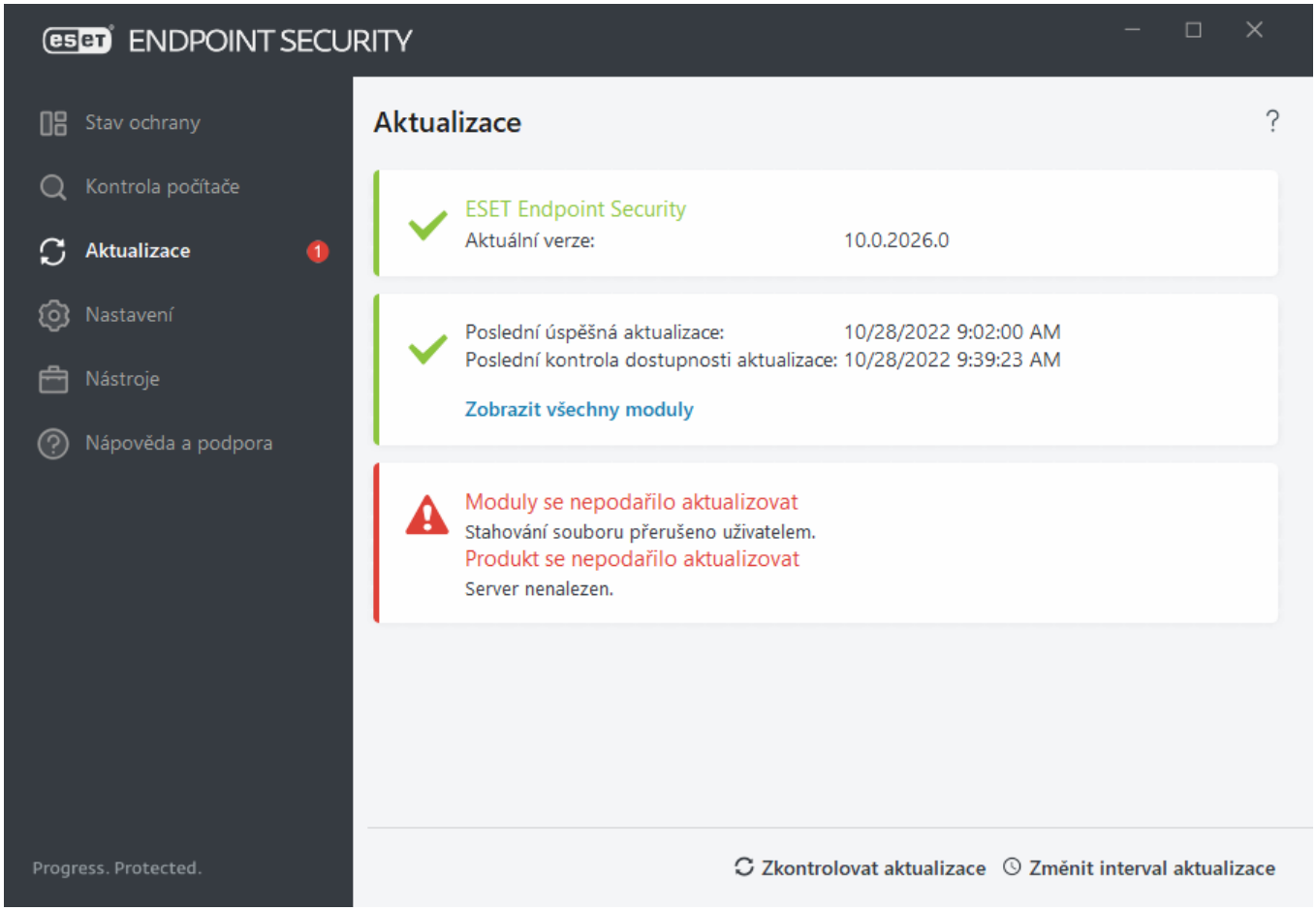
Za normálních okolností, při pravidelné a úspěšném stahování aktualizací, se v okně **Aktualizace** zobrazuje zelená fajfka. Pokud tomu tak není, program nepoužívá aktuální detekční moduly, čímž se zvyšuje riziko infiltrace. V takovém případě doporučujeme co nejdříve moduly aktualizovat.

Poslední úspěšná aktualizace

Detekční jádro není aktuální – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci modulů. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Mezi nejčastější důvody patří nesprávně zadaná ověřovací data nebo nesprávně nastavené připojení k internetu.

S výše uvedeným chybovým hlášením souvisí i následující dvě hlášení o **neúspěšné aktualizaci modulů**:

1. **Neplatný licenční klíč** – vaše licence není aktivní. V dialogovém okně klikněte na příslušnou nabídku. Volbu potrvďte kliknutím na **Pokračovat**.
2. **Chyba při stahování aktualizačních souborů** – při pokusu o stažení aktualizačních souborů došlo k chybě. Doporučujeme, abyste vyzkoušeli připojení k internetu (otevřením jakékoli webové stránky ve webovém prohlížeči). Pokud se stránka nenačte, doporučujeme zkontrolovat, zda je internetové připojení správně nastaveno. Ujistěte se, že máte aktivní připojení k internetu od poskytovatele internetových služeb (ISP).



Pro více informací navštivte článek v ESET Databázi znalostí Aktualizace modulů nebyla úspěšná a skončila s chybou.

Jak vytvořit aktualizační úlohu?

Aktualizaci můžete provést ručně kliknutím na tlačítko **Zkontrolovat aktualizace** na záložce **Aktualizace** v hlavním okně programu.

Aktualizaci můžete také spouštět jako naplánovanou úlohu. Pro vytvoření naplánované úlohy klikněte v hlavním okně programu na záložku **Nástroje** > **Plánovač**. Ve výchozím nastavení jsou v ESET Endpoint Security aktivovány následující aktualizační úlohy:

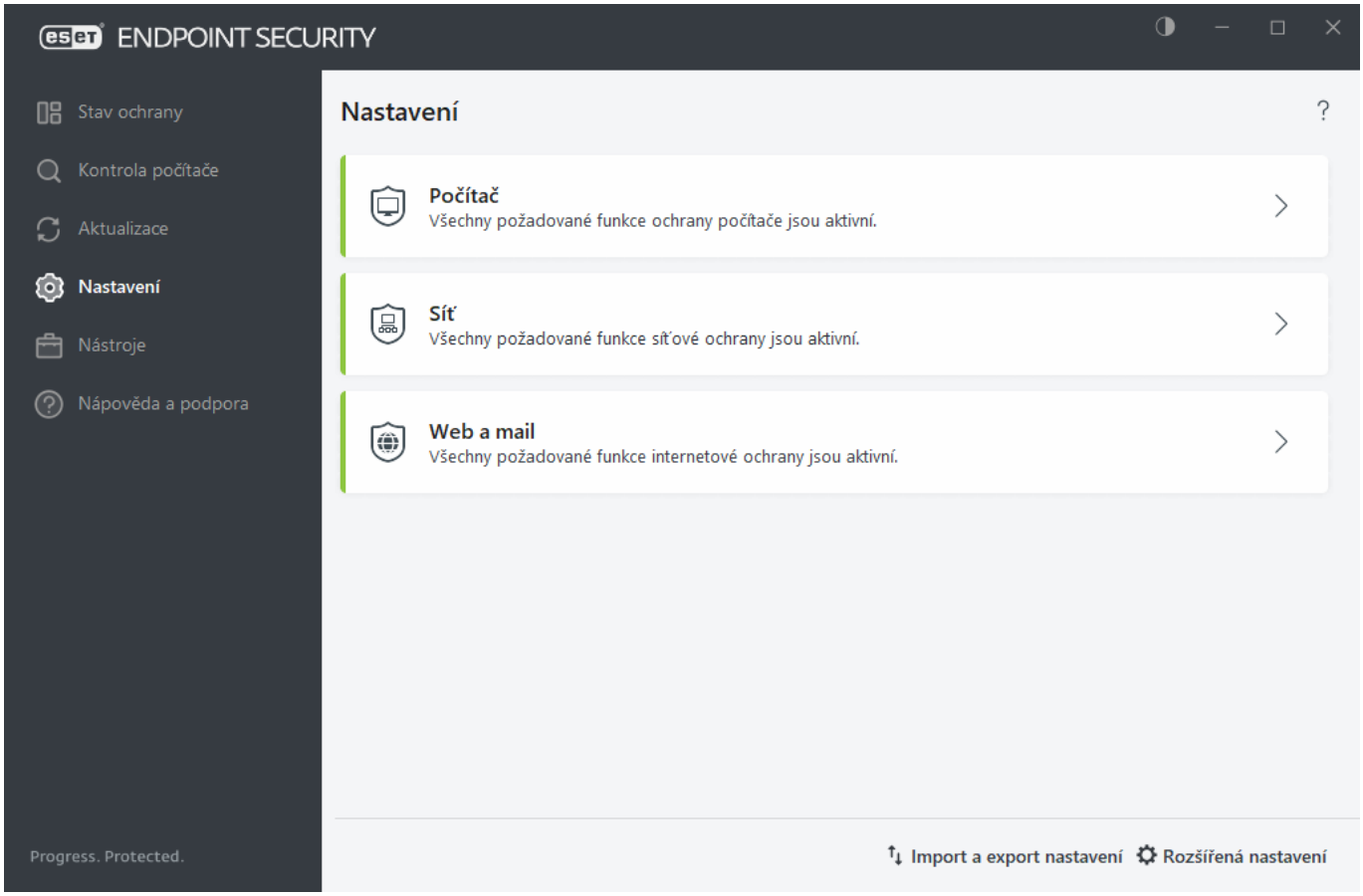
- **Pravidelná automatická aktualizace**,
- **Automatická aktualizace po přihlášení uživatele**,

Každou z uvedených aktualizačních úloh můžete upravit podle svých představ. Kromě standardních aktualizačních úloh můžete vytvořit nové aktualizační úlohy s vlastním nastavením. Podrobněji se vytváření a nastavení aktualizačních úloh zabýváme v kapitole Plánovač.

Nastavení

Dostupné ochranné funkce najdete v hlavním okně programu > **Nastavení**.

Při vytváření politiky v ESET PROTECT Web Console můžete u každého nastavení definovat příznak. Nastavení s příznakem má prioritu a nemůže být přepsáno pozdější politikou (pouze pokud obsahuje poslední politika příznak). To zajišťuje, aby nastavení nebylo změněno (např. uživatelem nebo pozdější politikou během slučování). Pro více informací o příznacích se podívejte do online nápovědy k ESET PROTECT.



Záložka **Nastavení** obsahuje následující sekce:

Počítač

Síť

Web a mail

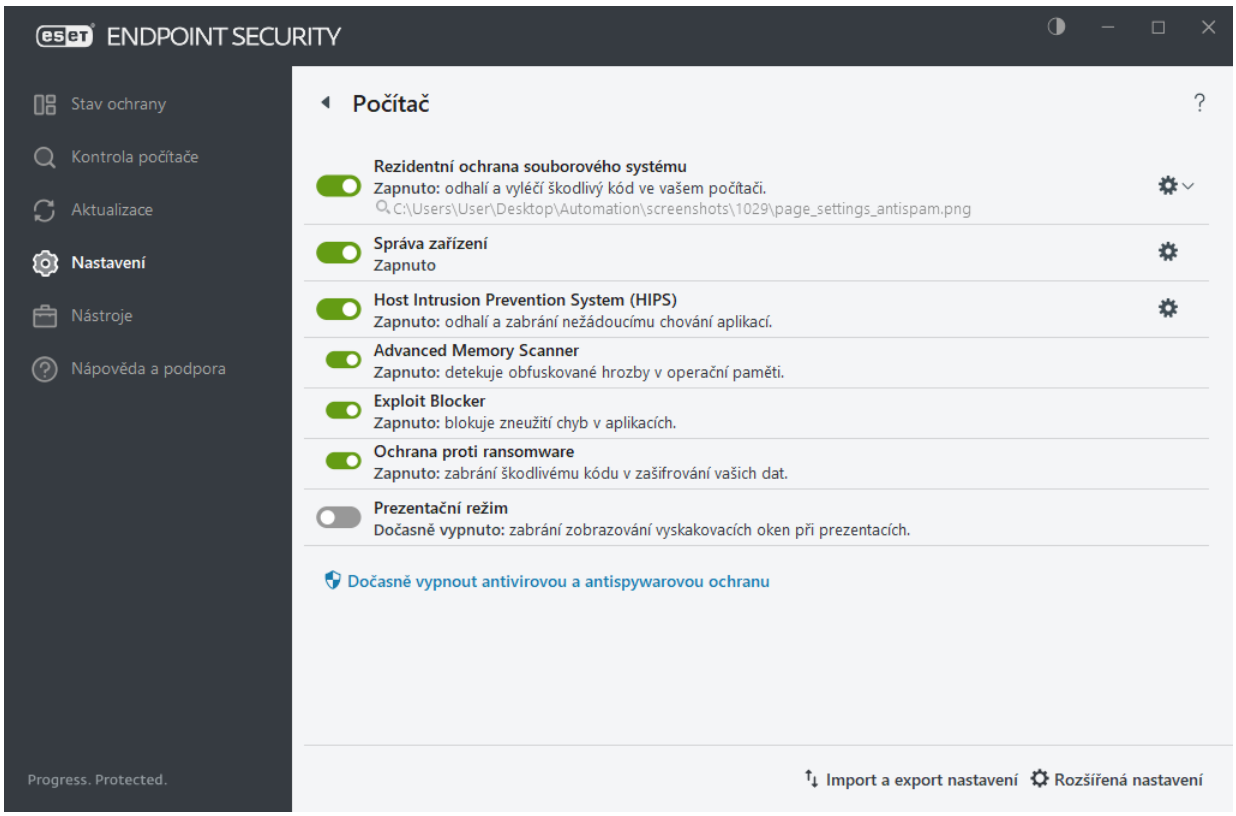
U modulu, jehož nastavení (zapnuto/vypnuto) máte definováno prostřednictvím ESET PROTECT politiky, se zobrazí ikona zámku. Nastavení takové komponenty aplikované politikou z ESET PROTECT může změnit pouze autentifikovaný uživatel z Active Directory (například přihlášený administrátor) nebo uživatel, který zná odpovídající heslo. Více informací o dočasné změně nastavení naleznete v online dokumentaci ESET PROTECT.

Pokud vypnete výše uvedeným způsobem jednotlivý bezpečnostní modul, automaticky se znovu zapne po restartování počítače.

Pro přístup do rozšířených možností nastavení klikněte na ozubené kolečko v dolní části. Kliknutím na Rozšířená nastavení můžete nakonfigurovat podrobnější parametry pro každý modul. Pomocí Import a export nastavení načtete parametry nastavení z již existujícího konfiguračního souboru ve formátu .xml nebo uložíte aktuální nastavení do konfiguračního souboru.

Počítač

Kliknutím na položku **Počítač** v hlavním okně programu > **Nastavení** zobrazíte přehled všech modulů ochrany:



V sekci **Počítač** můžete zapnout nebo vypnout následující komponenty:

- Rezidentní ochrana souborového systému – všechny soubory jsou kontrolovány v momentě, kdy je vytvoříte, otevřete nebo spustíte, Kliknutím na ozubené kolečko vedle položky Rezidentní ochrana souborového systému a následně na Upravit výjimky se zobrazí dialogové okno pro vytvoření výjimek, pomocí kterého můžete vyloučit soubory nebo složky z kontroly. Pro zobrazení a konfiguraci detailních parametrů rezidentní ochrany vyberte možnost Nastavit.
- Správa zařízení – prostřednictvím tohoto modulu dokáže produkt omezit přístup k výměnným médiím (CD/DVD/USB/...). Tento modul umožňuje blokovat nebo rozšířit filtry či oprávnění a nastavujte uživatelská pravidla pro práci s médii.
- Host Intrusion Prevention System (HIPS) – systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně na základě pravidel předdefinovaných pravidel společností ESET,
- **Advanced Memory Scanner** – v kombinaci s blokováním zneužití bezpečnostních děr (Exploit Blocker) poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.
- **Blokovat zneužití bezpečnostních děr (Exploit Blocker)** – tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, PDF čtečky a komponenty Microsoft Office). Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.
- **Ochrana proti ransomware** – tato součást představuje další vrstvu do modulu HIPS. Pro správnou funkci ochrany proti ransomware je třeba mít zapnutý Reputační systém ESET LiveGrid®. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.
- Prezentační režim je funkce pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni oznámeními a chtějí minimalizovat veškeré nároky na zatížení procesoru. Zároveň hlavní okno změní barvu

na oranžovou a upozorní vás na potenciální bezpečnostní riziko.

Dočasně vypnout antivirovou a antispywarovou ochranu – pomocí této možnosti můžete kdykoli dočasně vypnout antivirovou a antispywarovou ochranu. Po kliknutí se zobrazí dialogové okno, ve kterém můžete vybrat z rozbalovacího menu časový interval, po který bude daný modul vypnut. Akci dokončete kliknutím na tlačítko **Použít**. Akci dokončete kliknutím na tlačítko **Použít**. Pro opětovnou aktivaci ochrany klikněte na **Zapnout antivirovou a antispywarovou ochranu**.

Chcete-li pozastavit nebo vypnout některé moduly ochrany, klikněte na ikonu .

Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.

Je detekována hrozba

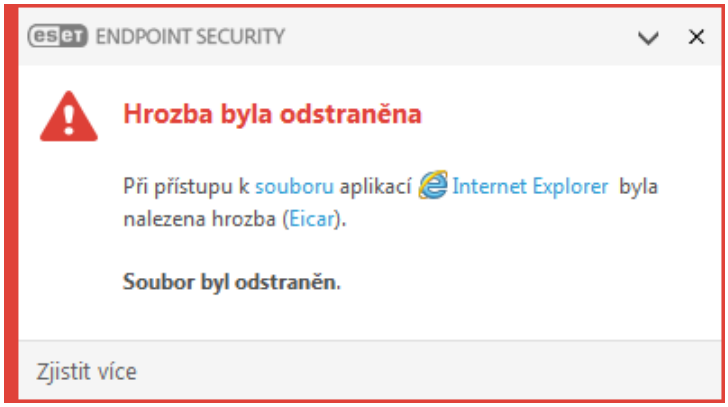
Infiltrace se mohou do počítače dostat z různých zdrojů: z webových stránek, ze sdílených složek, prostřednictvím e-mailu, z výměnných médií (USB, externí disků, CD a DVD jiných).

Standardní chování

ESET Endpoint Security dokáže zachytit infiltrace pomocí:

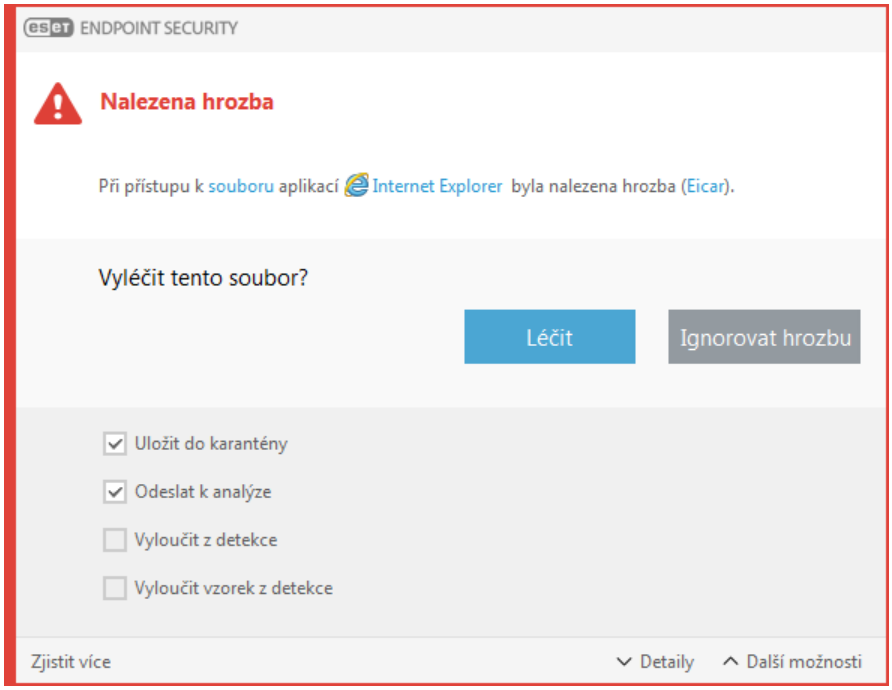
- Rezidentní ochrany souborového systému,
- Ochrana přístupu na web
- Ochrany poštovních klientů,
- Volitelné kontroly počítače.

Každý z těchto modulů používá standardní úroveň léčení. Program se pokusí soubor vyléčit a přesunout do Karantény, nebo přeruší spojení. Oznámení se zobrazují v pravé dolní části obrazovky. Pro více informací o detekovaných/vyléčených objektech přejděte do kapitoly Protokoly. Pro více informací o jednotlivých úrovních léčení a jejich chování si prosím přečtěte kapitolu Léčení.



Léčení a mazání

Pokud rezidentní ochrana nemá předdefinovanou akci pro daný typ souboru, zobrazí se dialogové okno s výběrem akce. Obvykle jsou dostupné možnosti **Léčit**, **Vymazat** a **Žádná akce**. Výběr možnosti **Žádná akce** nedoporučujeme, protože v tomto případě zůstane infekce nevyléčena. Výjimku tvoří případy, kdy jste si jisti, že je soubor neškodný a byl detekován chybně.



Léčení souboru je možné provést, pokud do zdravého souboru byla zavedena část, která obsahuje škodlivý kód. V tomto případě má smysl pokusit se infikovaný soubor léčit a získat tak původní zdravý soubor. V případě, že infiltrací je soubor, který obsahuje výlučně škodlivý kód, bude odstraněn.

Pokud je soubor uzamčen nebo používán systémovým procesem, bude obvykle odstraněn až po svém uvolnění, typicky po restartu počítače.

Obnovení z karantény

Karanténa je dostupná v hlavním okně programu ESET Endpoint Security na záložce **Nástroje** > **Karanténa**.

Soubory v karanténě lze vrátit do původního umístění:

- K tomuto účelu použijte funkci **Obnovit**, která je k dispozici v místní nabídce kliknutím pravým tlačítkem myši na daný soubor v karanténě.
- Pokud je soubor označen jako potenciálně nechtěná aplikace, je povolena možnost **Obnovit a vyloučit z kontroly**. Viz také kapitolu Výjimky.
- V kontextovém menu se dále nachází možnost **Obnovit do…**, pomocí které můžete obnovit soubor na jiné místo než to, ze kterého byl původně smazán.
- Funkce obnovení není dostupná například pro soubory umístěné ve sdílené síťové složce pro čtení.

Více hrozeb

Pokud infikované soubory nebyly vymazány během kontroly počítače (nebo je Úroveň léčení nastavena na **Neléčit**), zobrazí se dialogové okno s výběrem akce.

Mazání souborů v archivech

Pokud je zjištěna infiltrace uvnitř archivu, bude archiv při standardní úrovni léčení odstraněn pouze v případě, že obsahuje pouze infikovaný soubor. Archiv nebude vymazán, pokud kromě infiltrace obsahuje také nezávadné soubory. Opatrnost je potřeba dodržovat při nastavení přísné úrovně léčení, kdy v tomto případě bude archiv vymazán, bez ohledu na to, zda jeho obsah tvoří také zdravé soubory.

Pokud se váš počítač chová podezřele nebo máte podezření, že je infikován (zamrzá, je pomalý atp.), postupujte podle následujících kroků:

- Otevřete hlavní okno programu ESET Endpoint Security a přejděte na záložku Kontrola počítače.
- Klikněte na **Smart kontrola** (bližší informace naleznete v kapitole Kontrola počítače).
- Po dokončení kontroly se zobrazí protokol, ve kterém je uveden počet zkontrolovaných, infikovaných a vyléčených souborů.

Pokud chcete zkontrolovat pouze vybranou část disku, klikněte na **Volitelná kontrola** a vyberte cíle, které chcete ověřit na přítomnost virů.

Síť

Otevřete hlavní okno programu > **Nastavení** > **Síť** a nakonfigurujte základní nastavení síťové ochrany nebo vyřešte problémy se síťovou komunikací.

Chcete-li pozastavit nebo vypnout některé moduly ochrany, klikněte na ikonu  .

Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.

Kliknutím na ikonu ozubeného kola vedle modulu ochrany přejdete do rozšířených nastavení.

Firewall – filtruje veškerou síťovou komunikaci na základě konfigurace ESET Endpoint Security.

Nastavit... – otevřou se Rozšířená nastavení firewallu , kde můžete nastavit, jak bude firewall zpracovávat síťovou komunikaci.

Dočasně vypnout firewall – opak k funkci pro blokování veškeré komunikace. Při použití této možnosti je filtrování komunikace firewallem úplně vypnuto a všechna příchozí i odchozí spojení jsou povolena. Pokud je filtrování síťové komunikace firewallem vypnuté, obnovíte jej kliknutím na **Zapnout firewall**.

Blokovat veškerou komunikaci — veškerá příchozí a odchozí komunikace je blokována bránou firewall. Použití této možnosti je vhodné při podezření na možná kritická bezpečnostní rizika, která vyžadují odpojení systému od sítě. Pokud je **komunikace zablokována**, obnovíte ji po kliknutí na **Povolit veškerou komunikaci**.

Automatický režim (pokud je aktivován jiný režim filtrování) – kliknutím provedete změnu režimu filtrování na automatický (za použití vámi nastavených pravidel).

Interaktivní režim – (pokud je aktivován jiný režim filtrování) – kliknutím provedete změnu režimu filtrování na interaktivní.

Ochrana proti síťovým útokům (IDS) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Veškerý provoz, který je považován za škodlivý, je blokován. ESET Endpoint Security vás upozorní na připojení k nechráněné bezdrátové síti nebo síti se slabou ochranou.

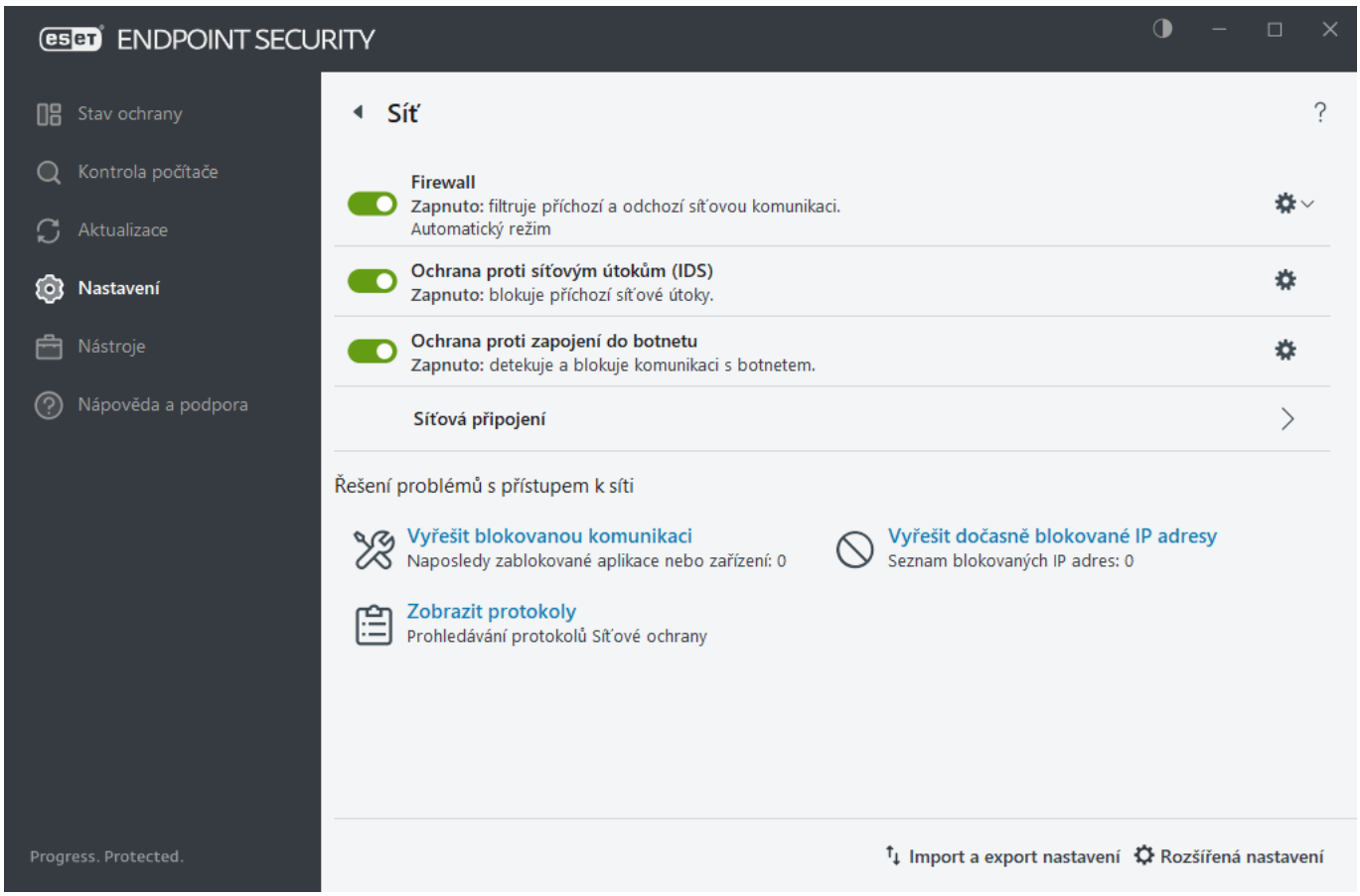
Ochrana proti zapojení do botnetu – rychlá a přesná identifikace škodlivého kódu v systému.

Síťová připojení – zobrazuje sítě, ke kterým jsou připojeny síťové adaptéry, s podrobnými informacemi.

Vyřešit blokovanou komunikaci – pomůže vám vyřešit problémy s připojením způsobené Firewallem. Podrobnější informace naleznete v Průvodci řešením problémů.

Vyřešit dočasně blokované IP adresy – zobrazí seznam IP adres, které byly detekovány jako zdroj útoků a přidány na blacklist pro blokování připojení po určitou dobu.

Zobrazit protokoly – otevře Protokol síťové ochrany.



Síťová spojení

V této části se zobrazí sítě, ke kterým jsou připojeny síťové adaptéry. Chcete-li zobrazit síťová připojení, otevřete hlavní okno programu > **Nastavení** > **Síťová ochrana** > **Síťová připojení**.

Dvojitým kliknutí na připojení v seznamu zobrazíte jeho podrobnosti a podrobnosti o síťovém adaptéru.

Najeďte na konkrétní síťové připojení a klikněte na ikonu nabídky ⋮ ve sloupci **Důvěryhodné** a vyberte jednu z následujících možností:

- **Změnit** – otevře okno Nastavení síťové ochrany, kde můžete přiřadit profil síťové ochrany konkrétní síti.
- **Zapomenout** – obnoví výchozí konfiguraci síťového připojení

Detaily síťového připojení

Dvojitým kliknutím na připojení v seznamu Síťová připojení zobrazíte jeho podrobnosti spolu s podrobnostmi o síťovém adaptéru. Podrobnosti o síťovém připojení a adaptéru vám pomohou identifikovat síť, kterou se snažíte nakonfigurovat v sekciOchrana síťového připojení.

Detaily síťového připojení:

- Stav síťového připojení
- Datum a čas první detekce sítě
- Kdy byla síť naposledy aktivní
- Celková doba připojení k této síti
- Profil síťového připojení
- Profil síťového připojení nastavený v systému Windows
- Konfigurace síťové ochrany (zda je síť důvěryhodná)

Podrobnosti o síťovém adaptéru:

- Typ připojení (kabelové, virtuální atd.)
- Název síťového adaptéru
- Popis adaptéru
- IP adresa společně s MAC adresou
- IPv4 a IPv6 adresa sítě s podsítí
- Přípona DNS
- IP adresa serveru DNS
- IP adresa serveru DHCP
- IP a MAC adresa výchozí brány
- Adresa MAC adaptéru

Řešení problémů s přístupem k síti

Tento průvodce vám pomůže při řešení problémů s připojením způsobených firewallem. **Řešení problémů s přístupem k síti** najdete v hlavním okně programu > **Nastavení** > **Síť** > **Vyřešit blokovanou komunikaci**.

Vyberte, zda chcete zobrazit komunikaci blokovanou pro **Lokální aplikace** nebo pro **Vzdálená zařízení**.

Nejprve z rozbalovacího menu vyberte časové období, ve kterém byla komunikace zablokována. Následně se zobrazí seznam zablokované komunikace konkrétní aplikace nebo zařízení společně s jejich reputací a počet blokování. Pro více informací o konkrétní komunikaci klikněte na možnost **Detaily**. Pokud se jedná o komunikaci, kterou potřebujete odblokovat, pokračujte dalším krokem.

Po kliknutí na tlačítko **Odblokovat** dojde k odblokování dříve blokované komunikace. Pokud se i nadále objevují problémy s aplikací nebo zařízení nefunguje podle očekávání, klikněte na **vytvořit jiné pravidlo** a veškerá komunikace, která byla dříve pro dané zařízení blokována, bude nyní povolena. Některá pravidla se uplatní až při dalším startu systému.

Kliknutím na **Otevřít pravidla firewallu** zobrazíte pravidla vytvořená průvodcem. Vytvořená pravidla si můžete kdykoli zobrazit v Rozšířených nastaveních > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Pravidla** > **Změnit**.

Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
- Add a firewall exception using the Troubleshooting wizard

Pokud pravidlo nelze vytvořit, zobrazí se chybová zpráva. Klikněte na **Zkusit znovu** a zopakujte proces odblokování komunikace nebo vytvořte další pravidlo ze seznamu blokované komunikace.

Seznam dočasně blokovaných IP adres

Pro zobrazení seznamu IP adres, ze kterých byly vedeny útoky, a proto byla komunikace z těchto adres dočasně zablokována, naleznete v hlavním okně programu ESET Endpoint Security na záložce **Nastavení** > **Síť** > **Seznam dočasně blokovaných IP adres**. IP adresy jsou dočasně blokovány po dobu jedné hodiny.

Sloupce

IP adresa – zablokovaná IP adresa.

Důvod blokování – typ útoku, kterému bylo zabráněno (například skenování portů).

Čas vypršení – doba, na jak dlouho bude komunikace z dané adresy blokována.

Ovládací prvky

Odstranit – kliknutím odstraníte ze seznamu vybranou dočasně blokovanou IP adresu.

Odstranit vše – kliknutím odstraníte ze seznamu všechny dočasně blokované IP adresy.

Přidat výjimku – kliknutím vytvoříte pro vybranou IP adresu IDS výjimku.

Protokoly síťové ochrany

Síťová ochrana ESET Endpoint Security ukládá důležité události do protokolu. Chcete-li zobrazit soubor protokolu, otevřete hlavní okno programu > **Nastavení** > **Síť** > **Zobrazit protokoly**.

Protokolování představuje účinný nástroj při odhalování chyb a zjišťování průniků do systému. Záznamy v protokolu síťové ochrany obsahují následující údaje:

- Datum a čas události
- Jméno události
- Zdroj
- Síťovou adresu cíle
- Síťový komunikační protokol
- Použité pravidlo nebo název červa, je-li identifikován
- Cesta a název aplikace
- Hash
- Jméno uživatele.
- Vystavitel aplikace (vydavatel)
- Název balíčku
- Název služby

Analyzováním těchto údajů můžete odhalit pokusy o narušení bezpečnosti systému. Příliš časté spojení z různých neznámých lokalit, hromadné pokusy o navázání spojení, komunikující neznámé aplikace či neobvyklá čísla portů mohou pomoci v odhalení potenciálního bezpečnostního rizika a minimalizaci jeho následků.

> **Zneužití zranitelnosti zabezpečení**
> Zpráva o zneužití bezpečnostní chyby je zaznamenána, i když je konkrétní zranitelnost již opravena. Děje se tak v případě, kdy je detekován a blokován pokus o zneužití na úrovni sítě ještě předtím, než ke zneužití dojde.

Řešení problémů se síťovou ochranou ESET

Pokud máte po nainstalování ESET Endpoint Security problémy s připojením, existuje několik způsobů, jak zjistit, zda problém způsobuje Síťová ochrana ESET. Síťová ochrana ESET vám navíc pomůže vytvořit nová pravidla nebo výjimky pro řešení problémů s připojením.

V následujících kapitolách naleznete možná řešení problémů souvisejících se Síťovou ochranu ESET:

- Řešení problémů s přístupem k síti
- Protokolování a vytváření pravidel nebo výjimek z protokolu
- Vytváření výjimek z oznámení firewallu
- Rozšířené protokolování síťové ochrany
- Řešení problémů s Kontrolou síťové komunikace

Protokolování a vytváření pravidel nebo výjimek z protokolu

Standardně ESET Firewall nezaznamenává všechna zablokovaná spojení. Pokud chcete vidět, co zablokovala Síťová ochrana, otevřete Rozšířená nastavení > **Nástroje** > **Diagnostika** > **Rozšířené protokolování** a zapněte **Aktivovat rozšířené protokolování síťové ochrany**. Pokud v protokolu naleznete spojení, které nechcete blokovat, stačí na něj kliknout pravým tlačítkem myši a z kontextového menu vybráním možnosti **Příště neblokovat podobné události** vytvořit IDS pravidlo. Mějte na paměti, že protokol všech zablokovaných spojení může obsahovat stovky záznamů a může být obtížné v něm najít konkrétní spojení. Po vyřešení problému nezapomeňte protokolování opět deaktivovat.

Pro více informací přejděte do kapitoly Protokoly.

> Protokolování můžete použít pro zjištění pořadí pravidel, ve kterých Síťová ochrana blokuje konkrétní spojení. Navíc z protokolu je možné vytvořit pravidlo přesně tak, jak jej potřebujete.

Vytvoření pravidla z protokolu

V nové verzi ESET Endpoint Security můžete pravidla vytvářet přímo z protokolu. V hlavním okně programu přejděte na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu vyberte možnost Síťová ochrana. Následně klikněte pravým tlačítkem myši na požadovaný záznam a z kontextového menu vyberte možnost **Příště neblokovat podobné události**. Zobrazí se oznámení s informací, že bylo vytvořeno pravidlo.

Abyste mohli vytvářet pravidla z protokolu, je nutné v ESET Endpoint Security provést následující nastavení:

1. V Rozšířených nastaveních > **Nástroje** > **Protokoly** nastavte **Zaznamenávat události od úrovně** na **Diagnostické**.
2. Aktivujte možnost **Upozornit na příchozí útoky využívající bezpečnostní zranitelnosti** v Rozšířených

nastaveních > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Další možnosti** > **Detekce útoků**.

Vytváření výjimek z oznámení firewallu

Poté, co ESET firewall detekuje škodlivou síťovou aktivitu, zobrazí na pracovní ploše upozornění s popisem události. Toto oznámení obsahuje odkaz, pomocí kterého si můžete zobrazit podrobnější informace o zablokované hrozbě, a zároveň umožňuje vytvořit výjimku pro danou událost.

> Pokud síťová aplikace nebo zařízení nesprávně implementuje síťové standardy, její komunikace může být odchycena modulem IDS. V takovém případě můžete přímo ze zobrazeného oznámení vytvořit v ESET firewallu výjimku pro takovou aplikaci nebo zařízení.

Rozšířené protokolování síťové ochrany

Tato funkce byla navržena ke komplexnímu sběru protokolů pro potřeby technické podpory ESET. Tuto možnost aktivujte výhradně na výzvu specialisty technické podpory ESET. Mějte na paměti, že se následně začne generovat velké množství dat a může dojít ke zpomalení počítače.

1. Otevřete Rozšířená nastavení > **Nástroje** > **Diagnostika** a zapněte **Aktivovat rozšířené protokolování síťové ochrany**.
2. Pokuste se znovu navodit problém.
3. Vypněte rozšířené protokolování síťové ochrany.
4. PCAP protokol vytvořený po aktivování rozšířeného protokolování síťové ochrany naleznete ve stejné složce jako diagnostické výpisy: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Řešení problémů s Kontrolou síťové komunikace

Pokud se vyskytnou problémy s prohlížečem nebo e-mailovým klientem, je třeba nejprve zjistit, zda za ně může Kontrola síťové komunikace. Zkuste dočasně vypnout Kontrolu síťová komunikace v Rozšířených nastaveních > **Detekční jádro** > **Kontrola síťové komunikace** (nezapomeňte kontrolu po dokončení opět zapnout, jinak váš prohlížeč a e-mailový klient zůstanou bez ochrany). Pokud problém po vypnutí filtrování zmizí, níže uvádíme seznam nejčastějším problémů a jejich řešení:

Problémy s aktualizací nebo zabezpečeným spojením

Pokud se aplikace nedokáže aktualizovat nebo komunikační kanál není zabezpečený:

- Pokud máte aktivní filtrování protokolu SSL/TLS, zkuste je dočasně vypnout. V případě, že to pomůže, ponechte filtrování protokolu SSL/TLS aktivní a vytvořte výjimku pro problematickou komunikaci: Deaktivace SSL/TLS. Znovu proveďte aktualizaci. Zobrazí se dialogové okno s informací o šifrované komunikaci. Ujistěte se, že se aplikace shoduje s tou, kterou řešíte, a že certifikát pochází ze serveru, ze kterého se aktualizuje. Následně vyberte možnost zapamatovat akci pro tento certifikát nebo klikněte na tlačítko Ignorovat. Pokud se již nezobrazí žádná další dialogová okna, přepněte režim filtrování zpět na automatický. Tím by měl být problém vyřešen.
- Pokud daná aplikace není prohlížečem nebo e-mailovým klientem, můžete ji zcela vyloučit z Ochrany přístupu na web (v případě prohlížeče nebo e-mailového klienta byste byli vystaveni nebezpečí). Všechny

aplikace, jejichž komunikace již byla v minulosti filtrována, by se měly zobrazit v seznamu aplikací, ve kterém je můžete vyloučit z filtrování protokolů. Ruční zadávání tedy není nutné.

Problémy s přístupem k síti

Pokud nejste schopni provádět žádné operace se síťovým zařízením (například zobrazit webovou stránku NAS nebo přehrávat video na domácím přehrávači), zkuste přidat IPv4 a IPv6 adresy na seznam vyloučených adres.

Problémy s konkrétní webovou stránkou

Pomocí správy adres URL můžete z Ochrany přístupu na web vyloučit konkrétní webové stránky. Například, pokud nemáte přístup k https://www.gmail.com/intl/en/mail/help/about.html, zkuste přidat *gmail.com* do seznamu adres vyloučených z filtrování.

Chyba: "Některé podporované aplikace pro import kořenového certifikátu stále běží“

Pokud máte aktivní SSL/TLS, ESET Endpoint Security zajistí, aby nainstalované aplikace důvěřovaly způsobu filtrování protokolu SSL tím, že do svého úložiště certifikátů importují certifikát. Některé aplikace mohou pro import certifikátu vyžadovat restart. V tomto případě se jedná o internetový prohlížeč Firefox a Opera. Ověřte, že žádný z nich není spuštěn (nejlépe to zjistíte tak, že otevřete Správce úloh a ujistíte se, že na kartě Procesy není firefox.exe ani opera.exe), a pak klikněte na Opakovat.

Neplatný vydavatel nebo podpis certifikátu

V tomto případě se import certifikátu nezdařil. Nejprve zkontrolujte, zda není spuštěna žádná z uvedených aplikací. Pak deaktivujte SSL/TLS a znovu jej aktivujte. Poté by již mělo dojít ke korektnímu importování.

Zablokována síťová hrozba

Tato situace může nastat, když je v systému zjištěn pokus o skenování portů, nebo když se aplikace ve vašem počítači pokouší přenést škodlivý provoz do jiného zařízení v síti nebo zneužít bezpečnostní díru.

V oznámení najdete typ hrozby a IP adresu příslušného zařízení. Po kliknutí na **Změnit zpracování této hrozby** se zobrazí následující možnosti:

Nadále blokovat – kliknutím zablokuje detekovanou hrozbu. Pokud chcete přestat dostávat oznámení o tomto typu hrozby z konkrétní vzdálené adresy, vyberte možnost **Neupozorňovat** před kliknutím na **Nadále blokovat**. Tím se vytvoří pravidlo modulu Intrusion Detection Service (IDS) s následující konfigurací: **Blokovat** – výchozí, **Oznámit** – ne, **Zapsat do protokolu** – ne.

Povolit - vytvoří pravidlo modulu Intrusion Detection Service (IDS), které povolí detekovanou hrozbu. Před kliknutím na **Povolit** vyberte jednu z následujících možností a zadejte nastavení pravidla:

- **Upozornit pouze při blokování této hrozby** – vytvoří se pravidlo s konfigurací: **Blokovat** – ne, **Oznámit** – ne, **Zapsat do protokolu** – ne.
- **Upozornit při každém výskytu této hrozby** – vytvoří se pravidlo s konfigurací: **Blokovat** – ne, **Oznámit** – výchozí, **Zapsat do protokolu** – výchozí.

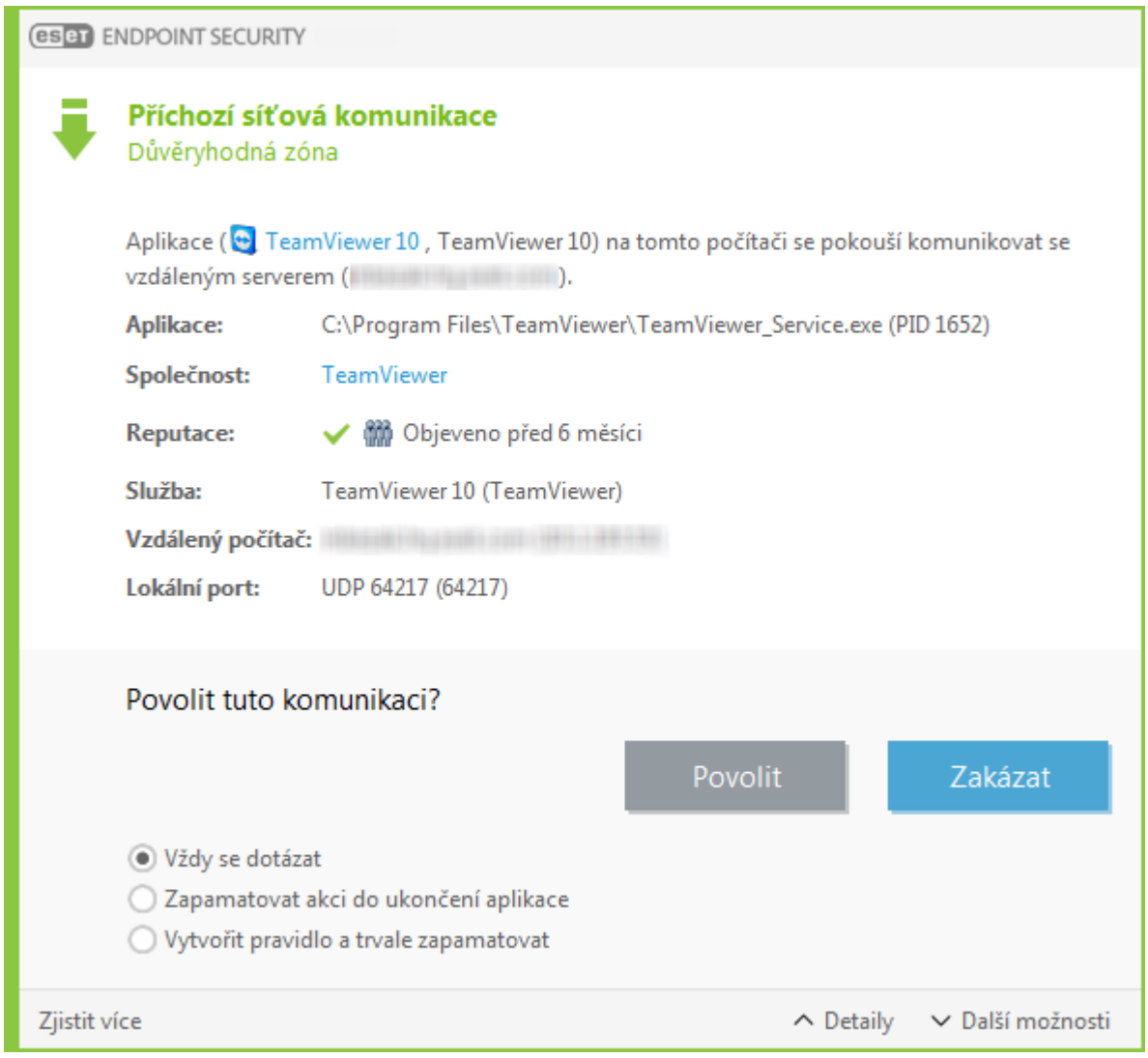
- **Neupozorňovat** – vytvoří se pravidlo s konfigurací: **Blokovat** – ne, **Oznámit** – ne, **Zapsat do protokolu** – ne.

Zobrazená informace se může lišit podle detekované hrozby.
Pro více informací o hrozbách a souvisejících pojmech přejděte do kapitoly Typy vzdálených útoků nebo Typy detekcí.
Pro vyřešení situace, kdy dochází k zobrazování upozornění na **Duplicitní IP adresu v síti**, se podívejte do naší Databáze znalostí.

Navazování spojení – detekce

Firewall detekuje každé nově vzniklé síťové spojení. Podle nastaveného režimu filtrování závisí, jaké činnosti pro toto nové spojení provede. Pokud je aktivován **Automatický** nebo **Administrátorský režim**, firewall provede předem určené akce bez interakce uživatele.

V případě **Interaktivního režimu** je zobrazeno informační okno, které oznamuje detekci nového síťového spojení spolu s informacemi o tomto spojení. Následně se rozhodněte, zda se chcete spojení **Povolit** nebo **Zakázat** (zablokovat). Pokud opakovaně povolujete stejné spojení, doporučujeme pro něj vytvořit pravidlo. To lze provést kliknutím na tlačítko **Vytvořit pravidlo a trvale zapamatovat**, kdy se akce vytvoří jako nové pravidlo firewallu. Pokud firewall v budoucnu rozpozná stejné spojení, pravidlo se uplatní automaticky bez nutnosti interakce uživatele.



Při vytváření nových pravidel povolujte pouze spojení, která znáte a považujete je za bezpečná. Firewall při

povolení všech spojení ztrácí svůj význam. Důležitými parametry spojení jsou zejména:

Aplikace – umístění spustitelného souboru a ID procesu. Nepovolujte připojení pro neznámé aplikace a procesy.

Vystavitel – jméno vydavatele aplikace. Kliknutím na text si zobrazíte bezpečnostní certifikát pro společnost.

Reputace – úroveň rizika připojení. Připojením je přiřazena úroveň rizika: V pořádku (zelené), neznámé (oranžové) nebo rizikové (červené) pomocí řady heuristických pravidel, která zkoumají charakteristiky každého připojení, počet uživatelů a čas prvního výskytu. Tyto informace se shromažďují pomocí technologie ESET LiveGrid®.

Služba – název služby, pokud je aplikace službou systému Windows.

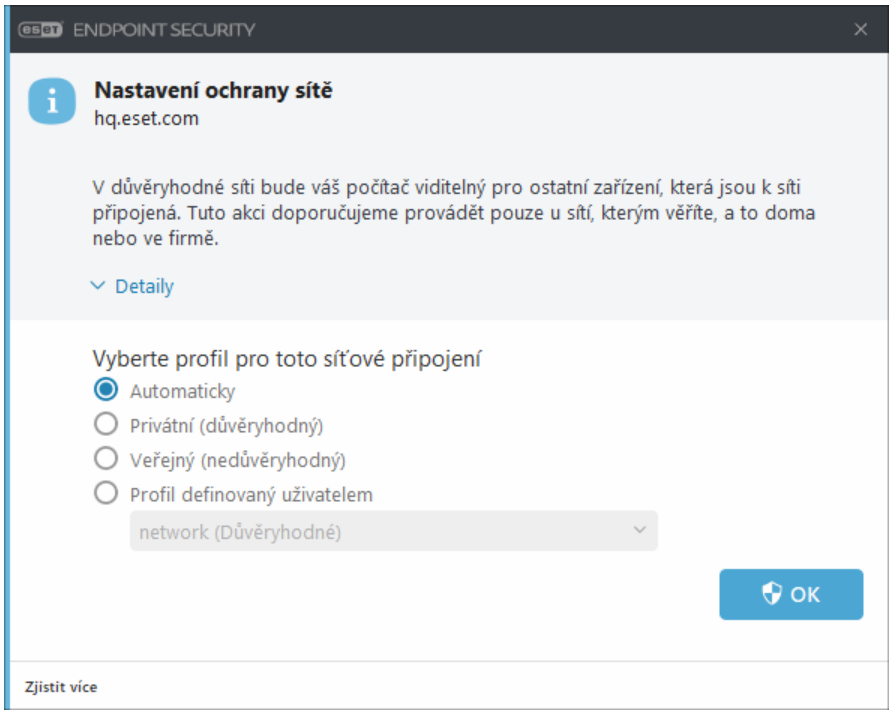
Vzdálený počítač – adresa vzdáleného zařízení. Povolujte pouze spojení na důvěryhodné a známé adresy.

Vzdálený port – komunikační port. Komunikace na známých portech (např. HTTP komunikace – port číslo 80.443) je obvykle bezpečná.

Počítačové infiltrace pro své šíření ve velké míře využívají internet a skrytá spojení, pomocí kterých jsou schopné infikovat systém. Správnou konfigurací pravidel firewallu je možné ochránit systém před proniknutím škodlivého kódu.

Zjištěno připojení do nové sítě

Ve výchozím nastavení převezme ESET Endpoint Security při detekci nového síťového připojení nastavení ze systému Windows. Chcete-li zobrazit dialogové okno při zjištění nové sítě, změňte Přiřazení profilu ochrany sítě na možnost **Zeptat se.** Konfigurace ochrany sítě se zobrazí vždy, když se počítač připojí k nové síti.



Můžete si vybrat z následujících profilů síťového připojení:

Automaticky – ESET Endpoint Security vybere profil automaticky na základě Spouštěčů nakonfigurovaných pro každý profil.

Privátní – pro důvěryhodné sítě (domácí nebo firemní síť). Vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti (přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít v bezpečných lokálních sítích. Tento profil je automaticky přiřazen síťovému připojení, pokud je nakonfigurováno jako doménová nebo privátní síť ve Windows.

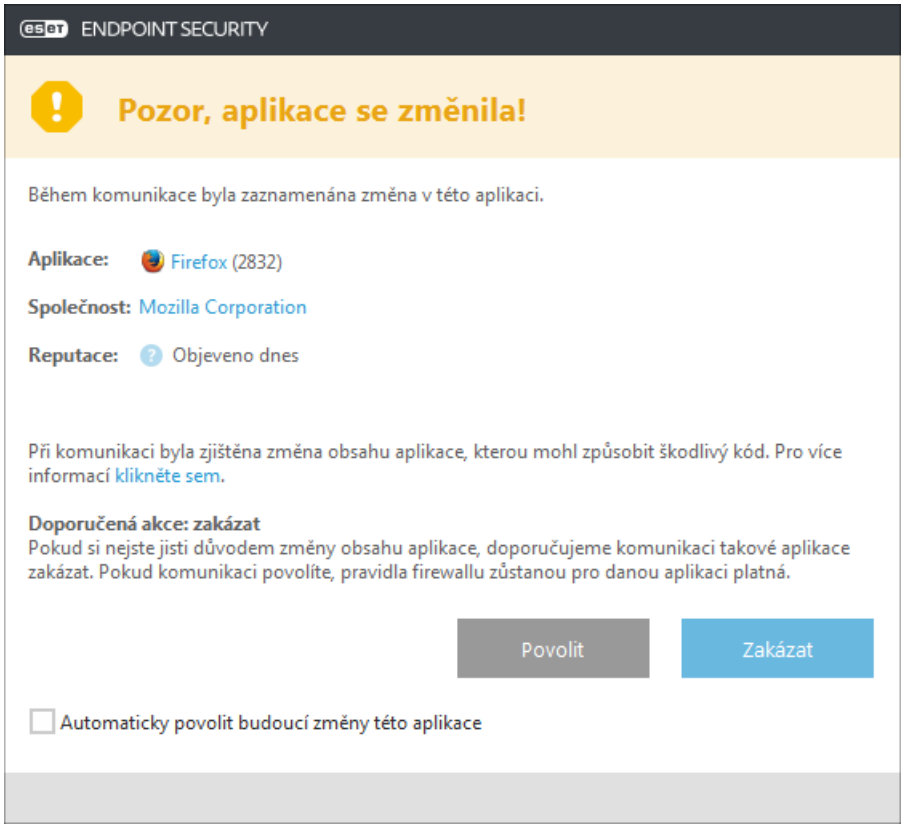
Veřejná – pro nedůvěryhodné sítě (veřejná síť). Soubory a složky uložené ve vašem počítači nebudou pro ostatní uživatele v síti dostupné, stejně tak nebude počítač viditelný v síti. Sdílení systémových prostředků bude deaktivováno. Toto nastavení doporučujeme při připojení k bezdrátovým sítím. Tento profil je automaticky přiřazen každému síťovému připojení, které není nakonfigurováno jako doménová nebo privátní síť ve Windows.

Profil definovaný uživatelem – z rozbalovacího menu můžete vybrat jeden z profilů, které jste vytvořili. Tato možnost je k dispozici pouze v případě, že jste vytvořili alespoň jeden vlastní profil.

⚠ Nesprávným nastavením sítě může být počítač ohrožen.

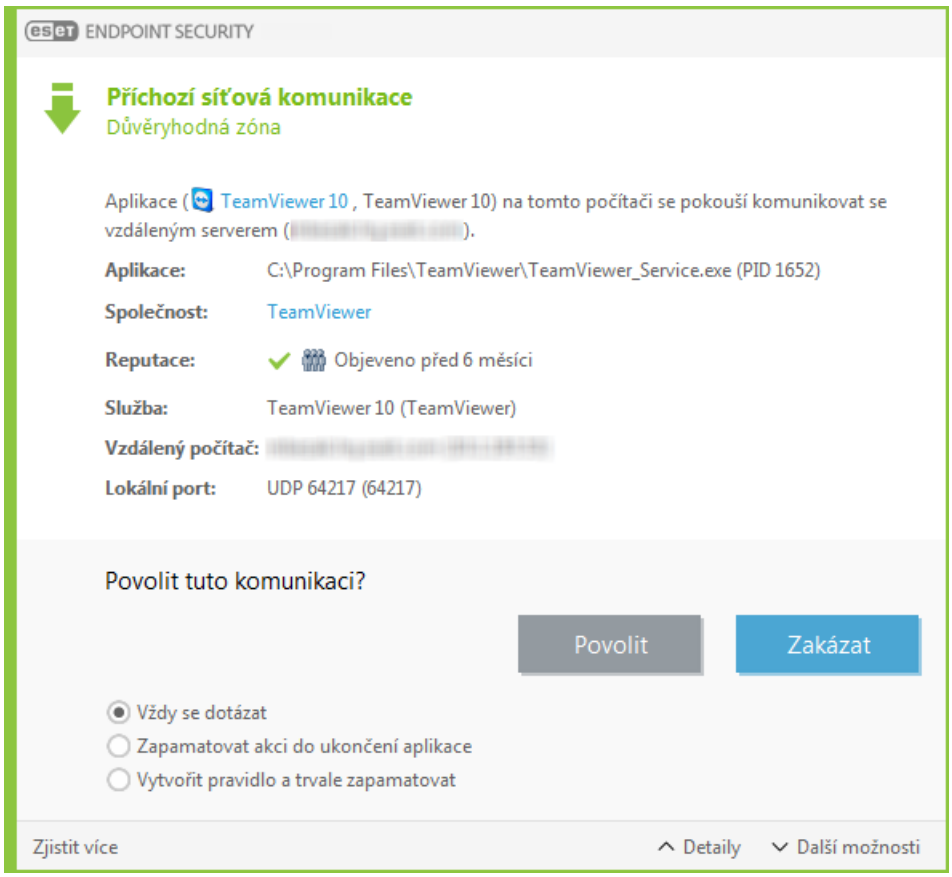
Změna aplikace

Firewall detekoval změnu aplikace, která již v minulosti navazovala komunikaci z počítače. Aplikace mohla být změněna například aktualizací na novější verzi. Ke změně aplikace mohlo také dojít infikováním nebezpečnou aplikací. Pokud si nejste jistí nutností změny v aplikaci, doporučujeme komunikaci aplikace zakázat a provést Kontrolu počítače s využitím aktuálního detekčního jádra. Pokud jste si jistí změnou této aplikace, můžete povolit jakoukoli změnu této aplikace vybráním možnosti **Automaticky povolit budoucí změny této aplikace** a vytvořit pro danou aplikaci výjimku.



Příchozí důvěryhodná komunikace

Příklad příchozí komunikace uvnitř důvěryhodné zóny:
Vzdálený počítač z důvěryhodné zóny se pokouší navázat spojení s aplikací běžící ve vašem počítači.



Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

Vystavitel – jméno vydavatele aplikace. Kliknutím na text si zobrazíte bezpečnostní certifikát pro společnost.

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

Vzdálený počítač – vzdálená strana, která se snaží navázat komunikaci.

Lokální port – port použitý pro komunikaci.

Vždy se dotázat – pokud je jako výchozí akce vybrána možnost **Dotázat se**, dialogové okno s výběrem akce se zobrazí při každém aplikování pravidla.

Zapamatovat do ukončení aplikace – ESET Endpoint Security si akci pro danou aplikaci zapamatuje do příštího restartu.

Vytvořit pravidlo a trvale zapamatovat – pokud zaškrtnete tuto možnost před povolením nebo zakázáním

komunikace, ESET Endpoint Security si akci zapamatuje a vytvoří pravidlo, které se uplatní při další komunikaci aplikace se vzdálenou stranou.

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí editoru pravidel firewallu.

Odchozí důvěryhodná komunikace

Příklad odchozí komunikace z důvěryhodné zóny:
Aplikace běžící na lokálním počítači se snaží připojit na jiný počítač v lokální síti, nebo síti která byla označena jako důvěryhodná.

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

Vystavitel – jméno vydavatele aplikace. Kliknutím na text si zobrazíte bezpečnostní certifikát pro společnost.

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

Vzdálený počítač – vzdálená strana, která se snaží navázat komunikaci.

Lokální port – port použitý pro komunikaci.

Vždy se dotázat – pokud je jako výchozí akce vybrána možnost **Dotázat se**, dialogové okno s výběrem akce se zobrazí při každém aplikování pravidla.

Zapamatovat do ukončení aplikace – ESET Endpoint Security si akci pro danou aplikaci zapamatuje do příštího restartu.

Vytvořit pravidlo a trvale zapamatovat – pokud zaškrtnete tuto možnost před povolením nebo zakázáním komunikace, ESET Endpoint Security si akci zapamatuje a vytvoří pravidlo, které se uplatní při další komunikaci aplikace se vzdálenou stranou.

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí editoru pravidel firewallu.

Příchozí komunikace

Příklad příchozí komunikace z internetu:
Vzdálený počítač se pokouší komunikovat s aplikací běžící na tomto počítači.

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

Vystavitel – jméno vydavatele aplikace. Kliknutím na text si zobrazíte bezpečnostní certifikát pro společnost.

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

Vzdálený počítač – vzdálená strana, která se snaží navázat komunikaci.

Lokální port – port použitý pro komunikaci.

Vždy se dotázat – pokud je jako výchozí akce vybrána možnost **Dotázat se**, dialogové okno s výběrem akce se zobrazí při každém aplikování pravidla.

Zapamatovat do ukončení aplikace – ESET Endpoint Security si akci pro danou aplikaci zapamatuje do příštího restartu.

Vytvořit pravidlo a trvale zapamatovat – pokud zaškrtnete tuto možnost před povolením nebo zakázáním komunikace, ESET Endpoint Security si akci zapamatuje a vytvoří pravidlo, které se uplatní při další komunikaci aplikace se vzdálenou stranou.

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí editoru pravidel firewallu.

Odchozí komunikace

Příklad odchozí komunikace z lokálního počítače do internetu:
Aplikace, která je spuštěna na lokálním počítači, se snaží připojit k internetu.

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

Vystavitel – jméno vydavatele aplikace. Kliknutím na text si zobrazíte bezpečnostní certifikát pro společnost.

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

Vzdálený počítač – vzdálená strana, která se snaží navázat komunikaci.

Lokální port – port použitý pro komunikaci.

Vždy se dotázat – pokud je jako výchozí akce vybrána možnost **Dotázat se**, dialogové okno s výběrem akce se zobrazí při každém aplikování pravidla.

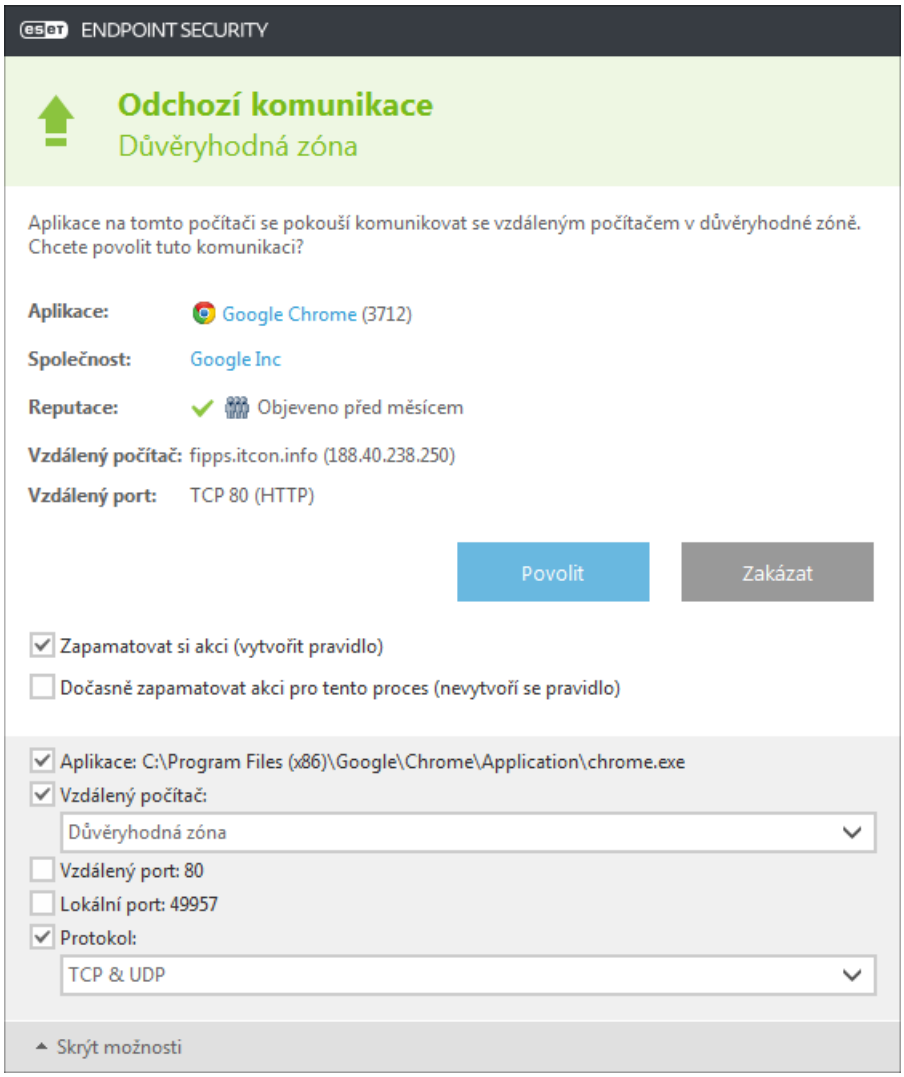
Zapamatovat do ukončení aplikace – ESET Endpoint Security si akci pro danou aplikaci zapamatuje do příštího restartu.

Vytvořit pravidlo a trvale zapamatovat – pokud zaškrtnete tuto možnost před povolením nebo zakázáním komunikace, ESET Endpoint Security si akci zapamatuje a vytvoří pravidlo, které se uplatní při další komunikaci aplikace se vzdálenou stranou.

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí editoru pravidel firewallu.



Možnosti zobrazení spojení

Kliknutím pravým tlačítkem na spojení se zobrazí následující možnosti:

Překládat IP adresy na názvy počítačů – je-li to možné, síťové adresy se uvádějí ve formě názvu DNS, nikoli v číselné podobě IP adresy,

Zobrazovat pouze TCP spojení – v seznamu spojení se zobrazí pouze ta, která patří k protokolu TCP.

Zobrazit naslouchající spojení – po vybrání této možnosti se zobrazí pouze spojení, ve kterých neprobíhá komunikace, ale port je v systému otevřený a čeká na spojení.

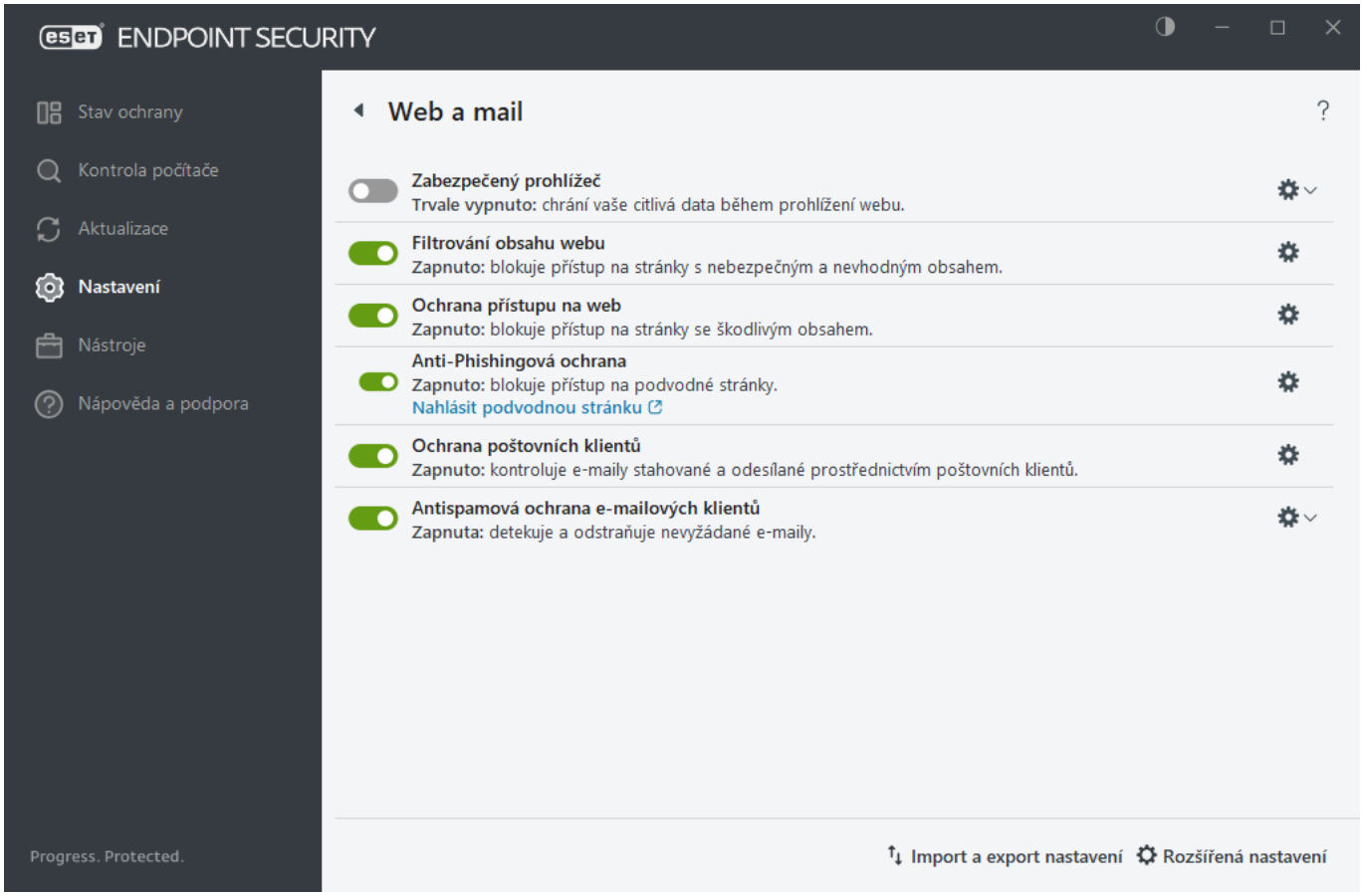
Zobrazit spojení v rámci počítače – tuto možnost vyberte, pokud chcete zobrazit pouze spojení, jejichž vzdáleným protějškem je lokální systém. Jedná se o spojení typu localhost.

Web a mail

Připojení k internetu je standardní funkcí v osobním počítači, ale také hlavním médiem pro přenos škodlivého kódu. Otevřete hlavní okno programu > **Nastavení** > **Web a mail** a nakonfigurujte funkce ESET Endpoint Security, které zvyšují internetovou ochranu.

Chcete-li pozastavit nebo vypnout některé moduly ochrany, klikněte na ikonu .

Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.



Kliknutím na ikonu ozubeného kola na řádku s modulem ochrany přejdete do jeho rozšířených nastavení.

Zabezpečený prohlížeč ochrání vaše citlivá data během prohlížení webu.

Modul **Filtrování obsahu webu** představuje užitečný nástroj pro administrátory, pomocí kterého mohou definovat sady pravidel za účelem omezení přístupu na webové stránky. Funkce Filtrování obsahu webu zabraňuje přístupu na stránky s nevhodným nebo škodlivým obsahem. Další informace naleznete v kapitole Filtrování obsahu webu.

Ochrana přístupu na web kontroluje komunikaci HTTP/HTTPS na přítomnost škodlivého kódu a phishingu.

Ochrana přístupu na web by měla být vypnuta pouze pro účely řešení problémů.

Anti-Phishingová ochrana umožňuje blokovat webové stránky, na kterých se nachází podvodný obsah. Doporučujeme ponechat anti-phishingovou ochranu zapnutou.

Nahlásit podvodnou stránku – odeslat phishingovou/škodlivou stránku společnosti ESET k analýze.

> Předtím, než odešlete stránku do společnosti ESET, se ujistěte, že splňuje alespoň jedno z níže uvedených kritérií:
> • Stránka není detekována jako škodlivá.
> • Stránka je chybně detekována jako škodlivá. V tomto případě nehlaste neoprávněně blokovanou stránku.

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3(S) a IMAP(S). Pomocí zásuvných modulů do/z poštovních klientů zajišťuje ESET Endpoint Security kontrolu veškeré komunikace.

Antispamová ochrana poštovních klientů filtruje nevyžádané e-mailové zprávy.

Pro nastavení **Antispamové ochrany poštovních klientů** klikněte na ikonu ozubeného kola a vyberte si z následujících možností:

- **Nastavit** – kliknutím si otevřete rozšířené nastavení antispamové ochrany poštovních klientů.
- **Uživatelský seznam adres** (pokud je povolen) – otevře dialogové okno, ve kterém můžete přidávat, upravovat nebo odstraňovat adresy a definovat tak antispamová pravidla; pravidla v tomto seznamu se použijí na aktuálního uživatele
- **Globální seznam adres** (pokud je povolen) - otevře dialogové okno, ve kterém můžete přidávat, upravovat nebo odstraňovat adresy a definovat tak antispamová pravidla; pravidla v tomto seznamu se použijí pro všechny uživatele

Anti-Phishingová ochrana

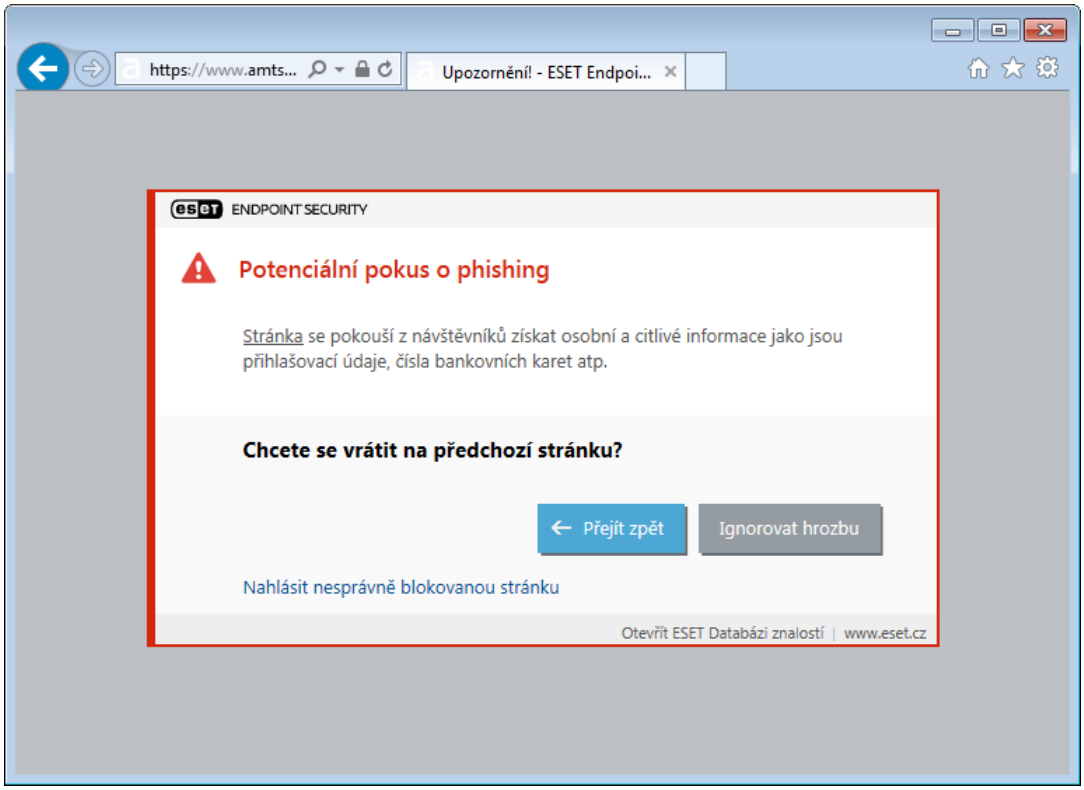
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem útočníků využívajících phishing je získání citlivých dat, jako jsou čísla bankovních účtů, PIN kódy a další. Více informací naleznete v glosáři. ESET Endpoint Security obsahuje anti-phishingovou ochranu, která blokuje internetové stránky s tímto obsahem.

Anti-Phishingová ochrana je ve výchozím nastavení zapnutá. Toto nastavení lze provádět v části Rozšířená nastavení > **Ochrany** > **Ochrana přístupu na web**.

Podrobnější informace o fungování Anti-Phishingové ochrany ESET Endpoint Security naleznete v ESET Databázi znalostí.

Přístup na stránky s phishingovým obsahem

Při přístupu na stránku se škodlivým obsahem se v internetovém prohlížeči zobrazí níže uvedené upozornění. Pokud přesto chcete stránku otevřít, klikněte na tlačítko **Ignorovat hrozbu** (nedoporučujeme).



V případě, že budete pokračovat na potenciální phishingovou stránku, na několik hodin se pro ni vytvoří výjimka. Následně bude přístup opět blokován. V části Rozšířená nastavení > **Ochrany** > **Ochrana přístupu na web** > **Správa URL adres** > **Seznam adres** > **Upravit** přidejte do seznamu webové stránky, které chcete upravit.

Nahlásit podvodnou stránku

Odkaz **Nahlásit nesprávně zablokovanou stránku** umožňuje nahlásit webovou stránku, která je nesprávně detekována jako hrozba.

Odkaz na webovou stránku můžete případně odeslat prostřednictvím e-mailové zprávy. E-mail odešlete na adresu samples@eset.com. Nezapomeňte vyplnit předmět e-mailu a přiložte maximální možné množství informací o dané stránce (jak jste se k ní dostali, od koho jste odkaz na ní obdrželi apod.).

Import a export nastavení

Na záložce **Nastavení** můžete do programu ESET Endpoint Security importovat nebo z něj naopak exportovat svou konfiguraci ze souboru ve formátu .xml.

Názorné ukázky

Pokud se chcete podívat na názornou ukázku, klikněte na návod ESET Databáze znalostí Jak importovat nebo exportovat nastavení bezpečnostního produktu ESET pomocí konfiguračního souboru .xml (článek nemusí být dostupný ve všech jazycích).

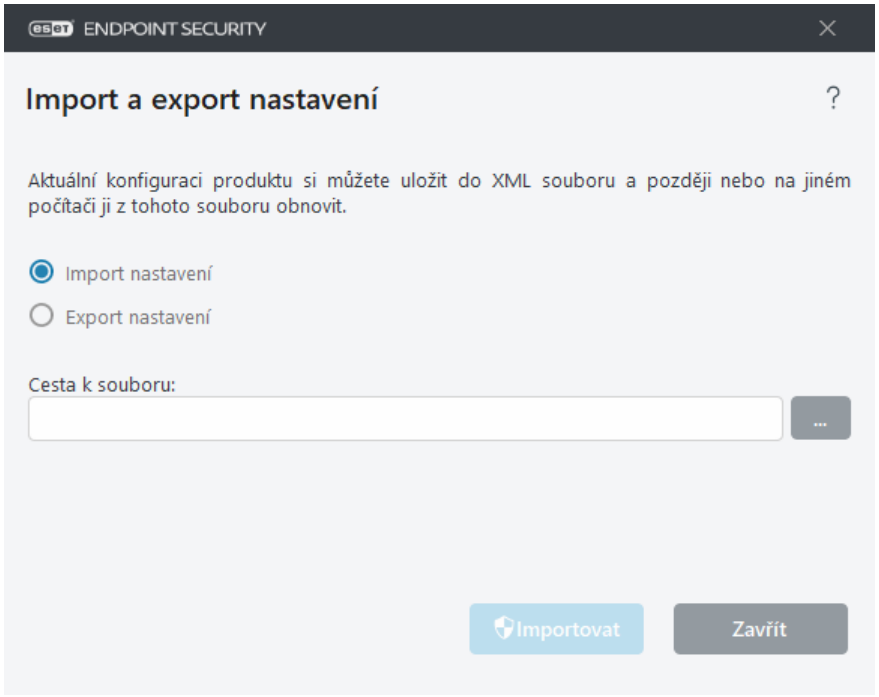
Importování a exportování nastavení je užitečné, například pokud si potřebujete zálohovat současné nastavení ESET Endpoint Security a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích. Stačí pouze naimportovat konfigurační .xml soubor.

Pro importování nastavení přejděte v hlavním okně programu na záložku **Nastavení**, klikněte na tlačítko **Import a**

export nastavení a v zobrazeném dialogovém okně vyberte možnost **Import nastavení**. Zadejte cestu k souboru s konfigurací, případně klikněte na **...** a najděte soubor, který chcete importovat.

V případě, že potřebujete uložit aktuální nastavení, v hlavním okně programu na záložce **Nastavení** klikněte na tlačítko **Import a export nastavení**. V zobrazeném dialogovém okně vyberte možnost **Export nastavení** a zadejte cestu k souboru. Případně kliknutím na **...** přejděte do umístění v počítači, do kterého chcete uložit soubor s konfigurací.

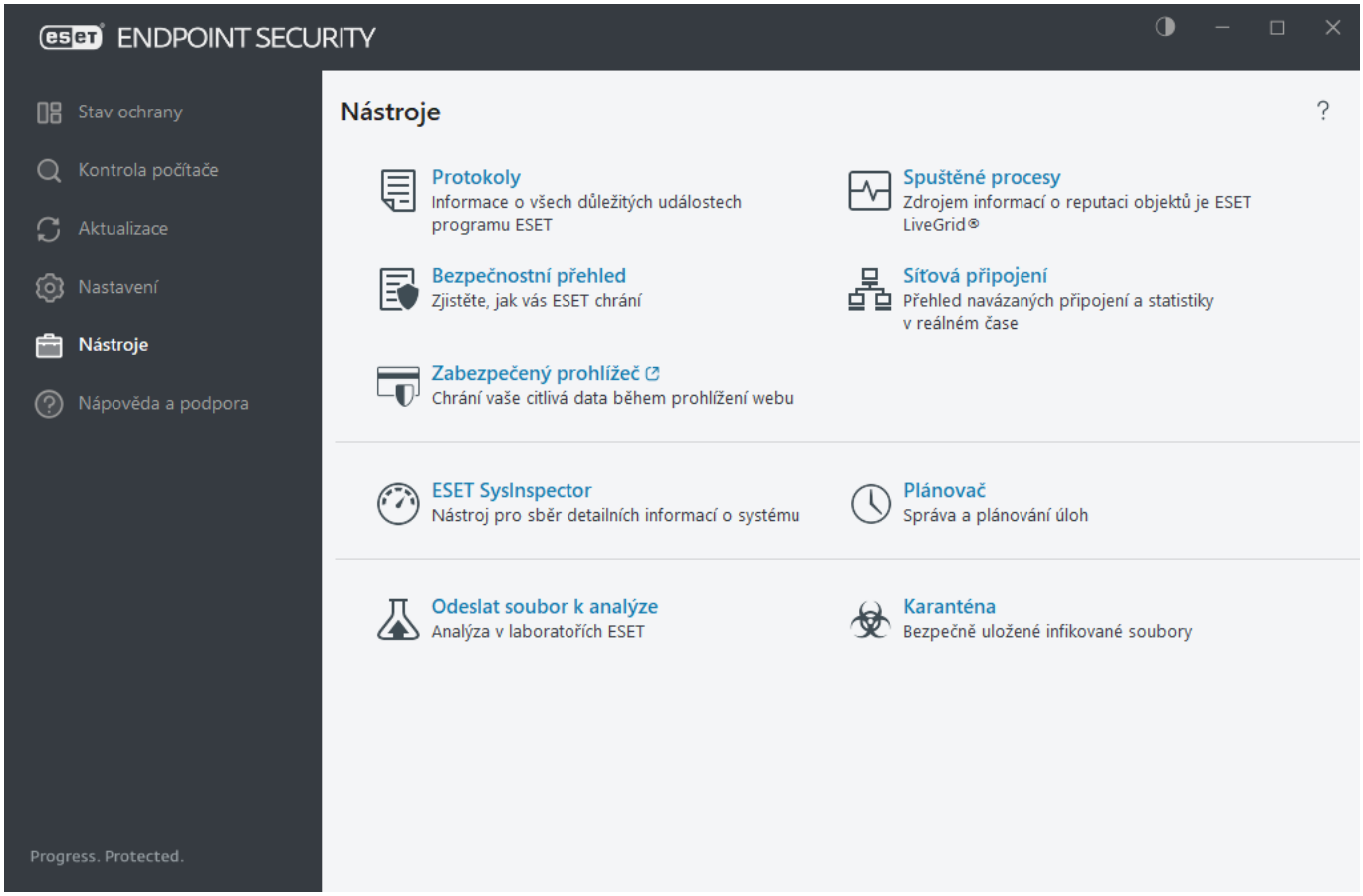
Pokud nemáte přístup pro zápis do zadané složky, může dojít k chybě při exportování nastavení.



Nástroje

Na záložce **Nástroje** naleznete součásti, které usnadňují správu programu a nabízejí rozšířené možnosti pro pokročilé uživatele.

- Protokoly
- Spuštěné procesy (tato součást se dostupná, pokud máte v produktu ESET Endpoint Security aktivní technologii ESET LiveGrid®)
- Bezpečnostní přehled (v nespravovaných prostředích)
- Síťová spojení (pokud je v produktu ESET Endpoint Security zapnutý firewall)
- ESET SysInspector
- Plánovač
- Odeslat soubor k analýze – umožní odeslat podezřelý soubor k analýze do ESET Research Lab (nemusí být k dispozici na základě vaší konfigurace ESET LiveGrid®)
- Karanténa



Protokoly

Do protokolů se zaznamenávají všechny důležité události programu, stejně tak v nich naleznete informace o detekovaných hrozbách. Protokolování představuje silný nástroj při systémové analýze, odhalování problémů a rizik a v neposlední řadě při hledání řešení. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové zprávy a protokoly si můžete prohlédnout přímo v rozhraní ESET Endpoint Security a v případě zájmu je archivovat. Protokoly je možné též v případě potřeby archivovat.

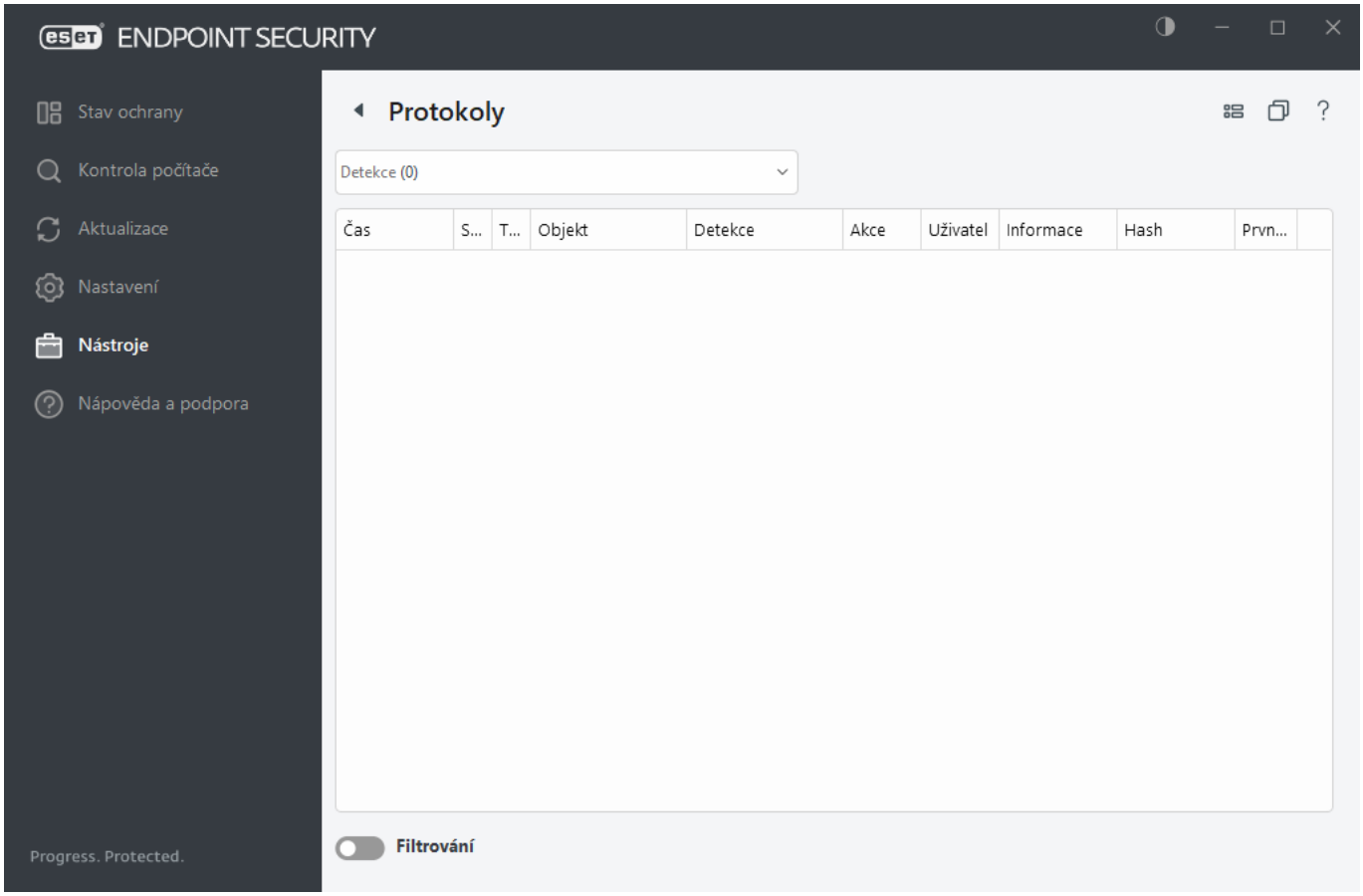
Protokoly naleznete v hlavním okně programu po kliknutí na záložku **Nástroje** > **Protokoly**. Následně z rozbalovacího menu **Protokoly** vyberte požadovaný typ protokolu. Dostupné jsou následující typy protokolů:

- **Detekce** – protokol zachycených detekcí a infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly programu ESET Endpoint Security. Informace zahrnují čas detekce, název infiltrace, umístění, provedenou činnost a uživatele přihlášeného v době detekce. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně. Nevyléčené infiltrace jsou vždy označeny červeně na světle červeném pozadí, neléčené infiltrace žlutě na bílém pozadí. Neléčené potenciálně nechtěné nebo zneužitelné aplikace jsou označeny žlutě na bílém pozadí.
- **Události** – protokol událostí obsahuje informace o všech událostech ESET Endpoint Security a chybách, které se vyskytly. Protokol událostí obsahuje informace o událostech a chybách, ke kterým v programu došlo. Informace z tohoto protokolu mohou administrátorům a uživatelům pomoci při hledání příčiny problémů, případně jejich řešení. Právě zde nejčastěji naleznete informace, které vám pomohou vyřešit problém vyskytující se v programu.
- **Kontrola počítače** – protokol kontroly počítače obsahuje výsledky dokončené ruční nebo naplánované kontroly. Každý řádek náleží samostatné kontrole. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.

- **Blokované soubory** – seznam souborů, k nimž produkt zablokoval přístup z důvodu využívání ESET Enterprise Inspector. V protokolu je uveden důvod blokace, modul, který přístup k souboru zablokoval, stejně jako uživatel a aplikace, prostřednictvím ní bylo k souboru přistupováno. Pro více informací se podívejte do online nápovědy k ESET Enterprise Inspector.
- **Odeslané soubory** – seznam souborů odeslaných k analýze do ESET LiveGrid® nebo ESET LiveGuard.
- **Audit** – každý záznam obsahuje informace o datu a čase provedené změny, jejím typu společně s popisem, zdrojem a informací o uživateli, který změnu provedl. Pro více informací přejděte do kapitoly Audit log.
- **HIPS** – protokoly obsahují záznamy konkrétních pravidel, která se mají zaznamenávat. V protokolu je zobrazena aplikace, která danou operaci vyvolala, výsledek (tzn. zda bylo pravidlo povoleno, nebo zakázáno) a název vytvořeného pravidla.
- **Zabezpečený prohlížeč** – obsahuje záznamy o nepotvrzených nebo nedůvěryhodných souborech načtených ve webovém prohlížeči.
- **Síťová ochrana** – protokol firewallu zobrazuje všechny vzdálené útoky detekované Ochranou proti síťovým útokům nebo Firewallem. Zde naleznete informace o jakémkoli útoku na váš počítač. Ve sloupci Událost se zobrazuje seznam útoků na vaše zařízení. Ve sloupci Zdroj se zobrazují podrobnější informace o útočníkovi. Ve sloupci Protokol naleznete komunikační protokol použitý při útoku. Analyzování tohoto protokolu pomůže včas odhalit pokusy o nepovolený průnik do vašeho systému. Pro více informací o síťových útocích přejděte do kapitoly IDS a pokročilé možnosti.

- **Filtrované webové stránky** – tento seznam je užitečný, pokud chcete zobrazit seznam webových stránek, které byly zablokovány Ochranou přístupu na web nebo Filtrováním obsahu webu. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.

- **Antispamovová ochrana poštovních klientů** – obsahuje záznamy související s e-mailovými zprávami, které byly označeny jako spam.
- **Filtrování obsahu webu** – protokol zobrazuje webové stránky, které byly zablokovány nebo povoleny, a do jaké kategorie patří. Ve sloupci Provedená akce naleznete informace o aplikovaném pravidle.
- **Správa zařízení** – obsahuje záznamy o výměnných médiích nebo zařízeních připojených k počítači. V protokolu se zobrazí pouze zařízení, na která byla aplikována pravidla Správce zařízení. Pokud nebylo na zařízení aplikováno žádné pravidlo, záznam v protokolu se nevytvoří. Pro každé zařízení se zobrazí také informace o typu zařízení, sériové číslo, název výrobce a velikost média (pokud jsou dostupné).



V každé sekci můžete jednotlivé události **kopírovat do schránky** přímo po označení události a kliknutím na tlačítko Kopírovat (nebo pomocí klávesové zkratky `Ctrl + Shift`). Pro výběr více záznamů podržte zároveň klávesy `Ctrl + C` a proveďte výběr.

Po kliknutí na přepínač **Filtrování** se zobrazí dialogové okno Filtrování protokolu, pomocí kterého můžete definovat kritéria filtrování.

V okně Protokoly můžete vyvolat kontextové menu kliknutím pravým tlačítkem myši na konkrétní záznam. Dostupné jsou následující možnosti:

- **Zobrazit** – po kliknutí si všechny záznamy protokolu zobrazíte v novém okně.
- **Filtrovat záznamy stejného typu** – po aktivovaní tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování,...).
- **Filtrovat...** – po kliknutí se otevře dialogové okno Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů.
- **Zapnout filtr** – kliknutím aktivujete filtr. Pokud jste dosud žádný filtr nedefinovali, zobrazí se průvodce jeho vytvořením. Při opětovném kliknutí se automaticky aktivuje naposledy použitý filtr.
- **Zrušit filtr** – kliknutím vypnete filtrování.
- **Kopírovat/Kopírovat vše** – po vybrání této možnosti zkopírujete všechny záznamy z daného okna.
- **Kopírovat buňku** – zkopíruje obsah buňky, na kterou jste v tabulce protokolů klikli pravým tlačítkem myši.
- **Odstranit/Odstranit vše** – kliknutím odstraníte vybrané/všechny záznamy – tato akce vyžaduje administrátorská oprávnění.
- **Exportovat** – po kliknutí uložíte vybrané záznamy do souboru v .XML formátu.
- **Exportovat vše** – po kliknutí uložíte všechny záznamy do .XML formátu.
- **Hledat.../Hledat další.../Hledat předchozí...** – po kliknutí můžete definovat kritéria pro konkrétní záznamy pomocí Filtrování protokolu.
- **Vytvořit výjimku** – kliknutím spustíte průvodce vytvořením detekční výjimky (tato možnost není dostupná

pro objekty detekované jako malware).

Filtrování protokolů

Pro definování kritérií filtrování v hlavním okně programu na záložce Nástroje > **Protokoly** klikněte na tlačítko **Filtrování**.

Díky funkci filtrování protokolů se snadněji zorientujete v zobrazených záznamech, a to zejména v situaci, kdy je záznamů více. Záznamy protokolu můžete zúžit, například pokud hledáte určitý typ události, stav nebo časové období. Záznamy protokolu lze filtrovat pomocí výběru určitých hodnot ve vyhledávání. Ve výsledcích se následně zobrazí hodnoty, které jsou pro nastavená kritéria relevantní.

Zadejte klíčové slovo, které chcete vyhledat, do pole **Hledat text**. Hledání můžete upřesnit volbami v rozbalovací nabídce **Hledat ve sloupcích**. Další volby si nastavte v rozbalovací nabídce **Typy záznamů**. V menu **Rozsah času** si nastavte období, z kterého chcete zobrazit výsledky. Pro zobrazení přesnějších výsledků vyberte možnost **Hledat pouze celá slova** a **Rozlišovat velká a malá písmena**.

Hledat text

Zadejte řetězec (slovo nebo jeho část). Následně se zobrazí pouze záznamy obsahující daný řetězec. Ostatní záznamy se přeskočí.

Hledat ve sloupcích

Tuto možnost použijte, pokud chcete vyhledávat klíčové slovo pouze v konkrétních sloupcích. Vybrat můžete jeden nebo více sloupců.

Typy záznamů

Z rozbalovacího menu si vyberte typy záznamy, které chcete zobrazit:

- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informační** – jedná se o informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíší kritické chyby, chybová a varovná hlášení.
- **Chyby** – kromě kritických varování se zaznamenají chyby typu "Chyba při stahování souboru aktualizace".
- **Kritické chyby** – zobrazí se pouze kritické chyby (chyba při startu antivirové ochrany

Časové období

Definujte časové období, za které chcete zobrazit výsledky:

- **Nedefinováno** (výchozí) – nebere v potaz datum a čas, prohledává se celý protokol.
- **Poslední den**
- **Poslední týden**
- **Poslední měsíc**
- **Vlastní** – filtrovány jsou výsledky v období definovaném pomocí možnosti Od: a Do:.

Hledat pouze celá slova

Vyberte tuto možnost, pokud chcete vyhledávat pouze slova tak, jak jste je zadali, a požadujete přesné výsledky.

Rozlišovat velká a malá písmena

Tuto možnost **zapněte**, pokud chcete při vyhledávání rozlišovat velikost písmen. Po dokončení konfigurace filtru pro vyhledávání v protokolu klikněte na tlačítko **OK**, případně Najít pro zahájení vyhledávání. Protokol se prohledává ze shora dolů a začíná se na aktuální pozici (zvýrazněném záznamu). Vyhledávání se zastaví na prvním vyhovujícím záznamu. Pro zobrazení dalšího výsledku vyhledávání stiskněte klávesu **F3**, případně v kontextovém menu vyberte možnost **Najít** a upravte parametry vyhledávání.

Audit

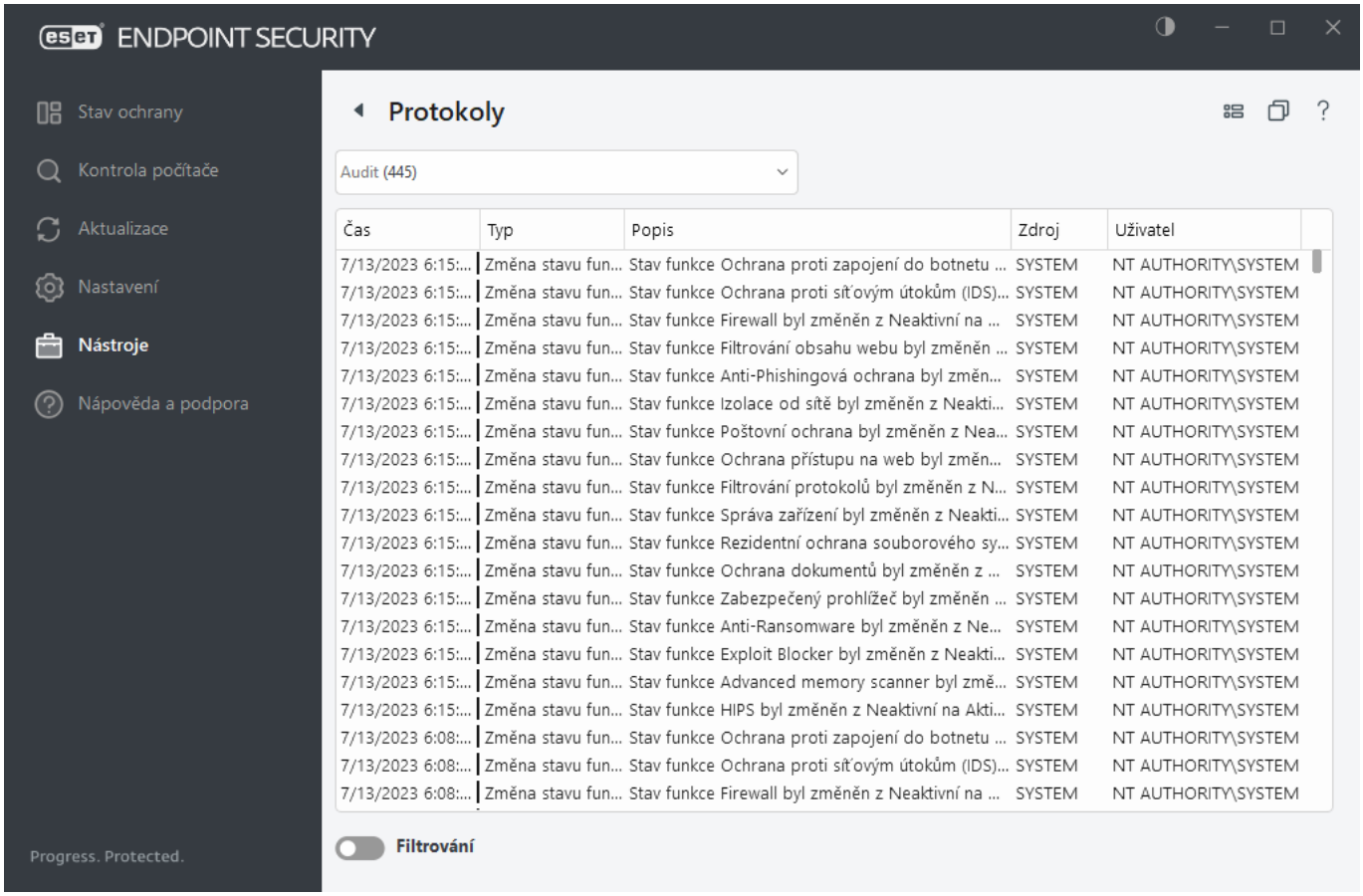
V enterprise prostředích má obvykle více uživatelů oprávnění pro konfiguraci bezpečnostních produktů. Protože změna konfigurace produktu může mít dramatický dopad na jeho fungování, je nezbytné, aby administrátoři měli k dispozici přehled o provedených změnách, který by mohli použít pro rychlou identifikaci problému, jeho vyřešení a zabránění výskytu stejného nebo podobného problému v budoucnu.

Audit log představuje nový typ protokolování. Jedná se o řešení, které může pomoci při identifikaci zdroje problému. Do audit logu se zaznamenávají provedené změny v konfiguraci nebo případně stavech ochrany, a vytvářejí se obrazy konfigurací pro porovnání změn.

Pro zobrazení **Audit logu** klikněte v hlavním okně programu na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu vyberte možnost **Audit**.

Audit log obsahuje následující informace:

- Čas – informace, kdy byla změna provedena
- Typ – jaké nastavení nebo funkce byla změněna
- Popis – co konkrétně, a jaká část nastavení, byla změněna společně s počtem změněných položek
- Zdroj – kdo inicializoval změnu
- Uživatel – pod nímž byla změna provedena



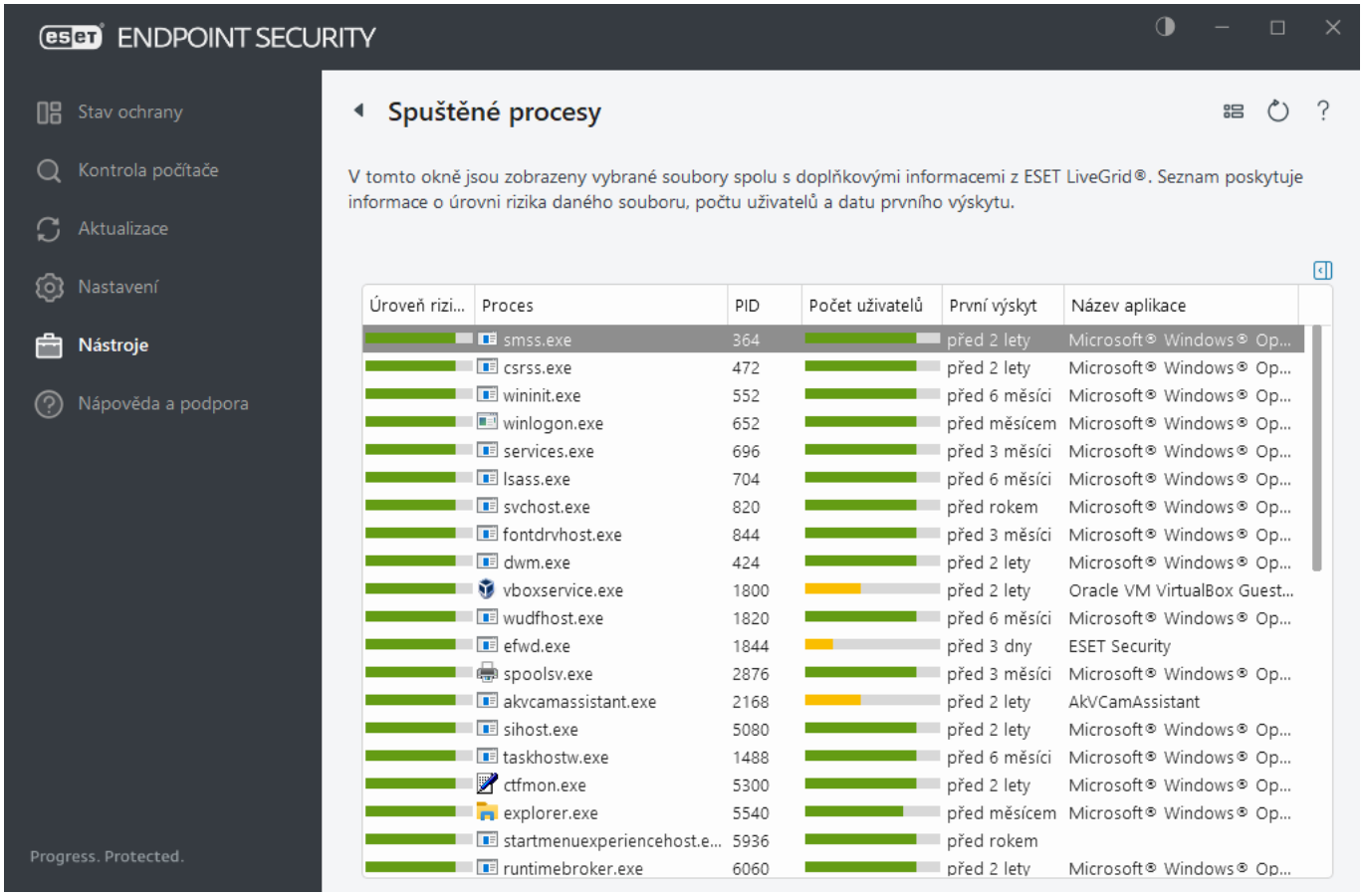
Pro zobrazení detailních informací o provedené změně klikněte v hlavním okně programu na záložce **Nástroje** > **Protokoly** > Audit pravým tlačítkem myši na zobrazený záznam a z kontextového menu vyberte možnost Zobrazit změny. V případě potřeby můžete nastavení **Obnovit** (tato možnost není dostupná pro produkty spravované prostřednictvím ESET PROTECT). Po vybrání možnosti Odstranit vše se do protokolu zapíše informace o provedené akci.

Pokud máte v **Rozšířeném nastavení** > Nástroje > **Protokoly** aktivní možnost **Automaticky optimalizovat protokoly**, Audit log se bude automaticky defragmentovat, stejně jako ostatní protokoly.

Pokud máte v **Rozšířeném nastavení** > Nástroje > **Protokoly Automaticky vymazat záznamy starší než (dní)**, záznamy starší než zadaný počet dní budou odstraněny.

Spuštěné procesy

Tento nástroj zobrazuje spuštěné programy a procesy a umožňuje společnosti ESET získávat informace o nových infiltracích. ESET Endpoint Security poskytuje detailnější informace o spuštěných procesech díky technologii ESET LiveGrid® pro zajištění lepší ochrany uživatelů.



Reputace – ve většině případů přiřazuje ESET Endpoint Security objektům (souborům, procesům, klíčům registru apod.) úroveň rizika pomocí technologie ESET LiveGrid® na základě heuristických pravidel a kontroly každého objektu na přítomnost škodlivého kódu. Poté na základě těchto výsledků přidělí procesům úroveň rizika od 9 – Nejlepší reputace (zelený) až po 0 – Nejhorší reputace (červený).

Proces – název aplikace nebo procesu, který aktuálně běží na počítači. Pro zobrazení všech běžících programů na počítači můžete použít také Správce úloh systému Windows. Správce úloh spustíte kliknutím pravým tlačítkem na Hlavní panel a vybráním možnosti **Spustit správce úloh**, případně pomocí klávesové zkratky **Ctrl** + **Shift** + **Esc**.

PID – ID běžícího procesu v operačním systému Windows.

Známé aplikace označené zeleně a jsou považovány za důvěryhodné. Proto pro zvýšení výkonu rezidentní ochrany a volitelné kontroly počítače nebudou kontrolovány.

Počet uživatelů – počet uživatelů, kteří používají danou aplikaci. Tyto informace se shromažďují pomocí technologie ESET LiveGrid®.

První výskyt – doba, kdy byl proces poprvé objeven pomocí technologie ESET LiveGrid®.

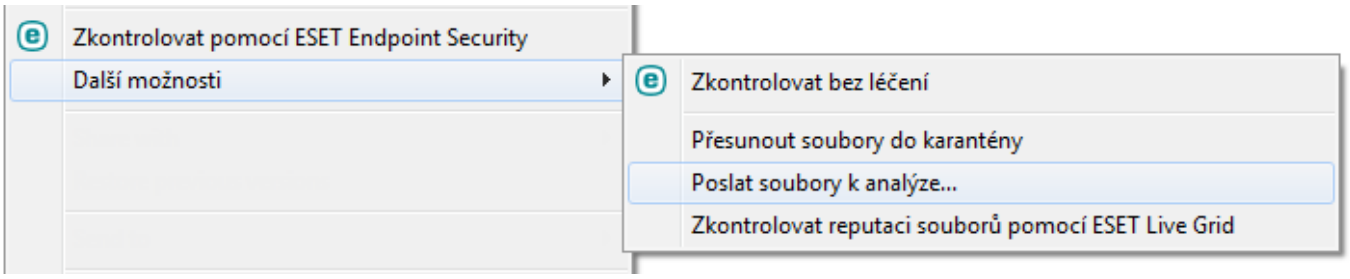
I v případě, že je aplikace označená jako Neznáma (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete soubor odeslat k analýze do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde o aplikaci obsahující škodlivý kód, její detekce bude zahrnuta do další aktualizace detekčního jádra.

Název aplikace – název aplikace nebo procesu.

Po kliknutí na jednotlivé aplikace se v dolní části okna zobrazí následující informace:

- **Cesta k souboru** – umístění aplikace v počítači,
- **Velikost souboru** – velikost souboru v kB (bajtech) nebo MB (megabajtech),
- **Popis souboru** – charakteristika souboru vycházející z jeho popisu získaného od operačního systému,
- **Název výrobce** – název výrobce aplikace nebo procesu,
- **Verze produktu** – tato informace pochází od výrobce aplikace nebo procesu,
- **Název produktu** – název aplikace, obvykle obchodní název produktu,
- **Vytvořeno** – datum a čas, kdy byla aplikace vytvořena,
- **Upraveno** – datum a čas, kdy byla aplikace naposledy upravena.

Reputaci můžete zjistit také pro soubory, které se nechovají jako spuštěné programy/procesy. Na soubor, který chcete zkontrolovat, klikněte pravým tlačítkem myši a ze zobrazeného kontextového menu vyberte **Další možnosti** > **Zkontrolovat reputaci souborů pomocí ESET LiveGrid®**.



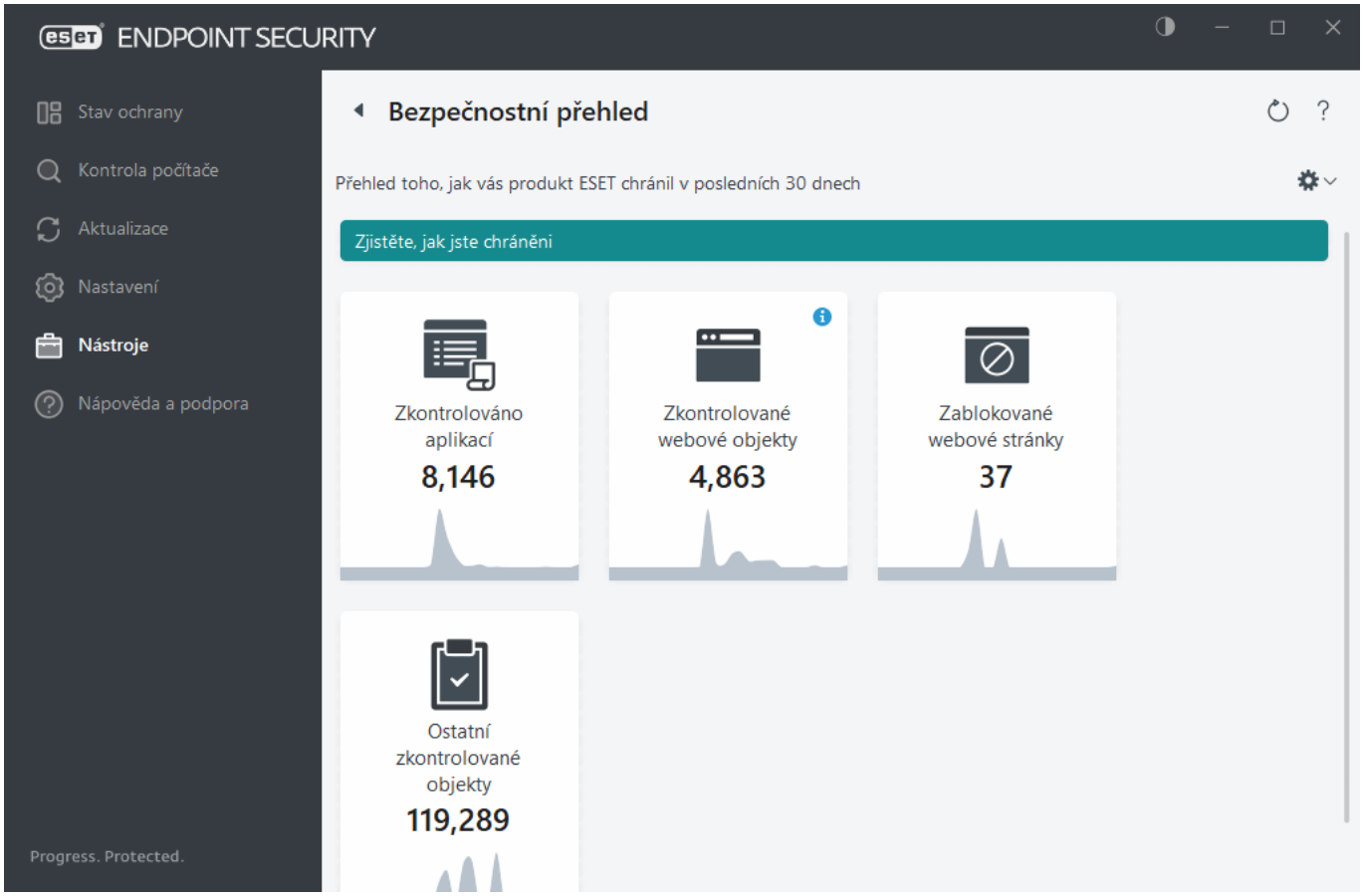
Bezpečnostní přehled

V této části naleznete statistické údaje o činnosti programu rozdělené do následujících kategorií:

- **Zablokováno webových stránek** – zobrazuje počet zablokovaných webových stránek (zablokováno na základě PUA, výskytu phishingu, hacknutého routeru, IP adresy nebo certifikátu).
- **Detekované infikované e-mailové objekty** – zobrazuje počet detekovaných infikovaných poštovních objektů.
- **Webové stránky zablokované Filtrováním obsahu webu** – zobrazuje počet stránek zablokovaných modulem Filtrování obsahu webu.
- **Detekované PUA** – zobrazuje počet detekovaných potenciálně nechtěných aplikací (PUA).
- **Detekovaných nevyžádaných e-mailů** – zobrazuje počet detekovaných spamů.
- **Zkontrolováno dokumentů** – zobrazuje počet zkontrolovaných dokumentů.
- **Zkontrolováno aplikací** – zobrazuje počet zkontrolovaných spustitelných objektů.
- **Ostatní zkontrolované objekty** – zobrazuje počet dalších zkontrolovaných objektů.
- **Zkontrolované objekty webových stránek** – zobrazuje počet zkontrolovaných objektů webových stránek.
- **Zkontrolované poštovní objekty** – zobrazuje počet zkontrolovaných poštovních objektů.

Pořadí výše uvedených kategorií se dynamicky mění. Na prvním místě jsou vždy zobrazeny kategorie s nejvyššími hodnotami. Kategorie obsahující nulové hodnoty se nezobrazují. Pro zobrazení dalších a skrytých kategorií klikněte na **Zobrazit více**.

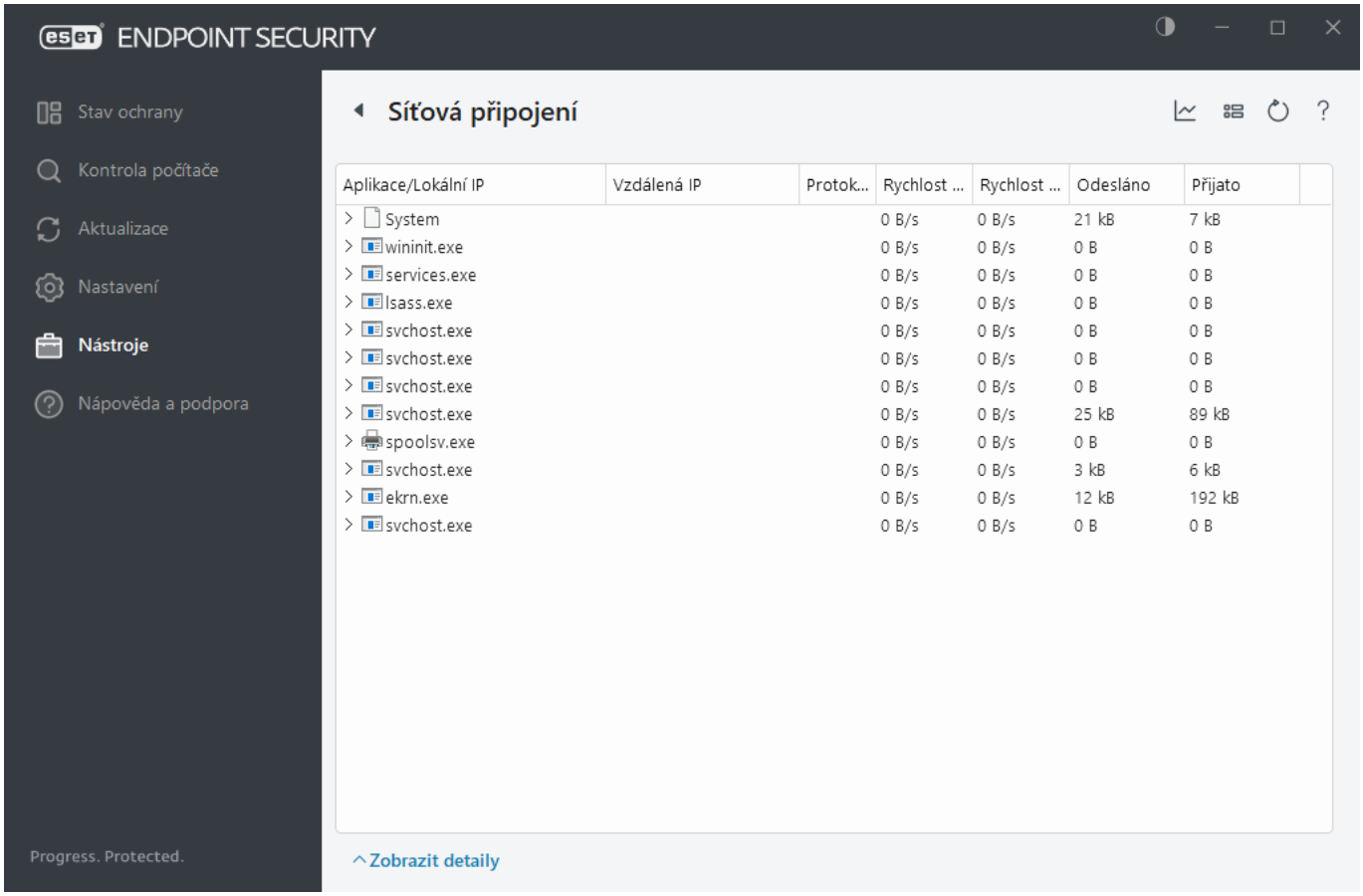
Kliknutím na ozubené kolečko v pravém horním rohu můžete **zapnout/vypnout upozornění na bezpečnostní přehled**, případně si zobrazit data za posledních 30 dní, resp. od aktivace produktu. Pokud jste produkt ESET Endpoint Security nainstalovali před méně než 30 dny, zobrazí se pouze data od instalace produktu. Výchozí dobou pro zobrazení dat je 30 dní.



Pomocí možnosti **Vynulovat data** odstraníte všechny statistiky a data z bezpečnostního přehledu. Tuto akci je nutné potvrdit, pokud toto nemáte v **Rozšířených nastaveních** (dostupných po stisknutí klávesy F5) definováno jinak v části Oznámení > **Interaktivní upozornění** > **Potvrzovací zprávy**.

Síťová spojení

V okně Síťová spojení je zobrazen seznam spojení, která jsou navázána, nebo čekají na navázání spojení. Tím získáte přehled o aplikacích, které komunikují se vzdálenou stranou.



Kliknutím na ikonu grafu si zobrazíte přehled síťové aktivity.

Na každém řádku je uveden název aplikace, aktuální rychlost přenášených dat a celkové množství přenesených dat. Seznam všech spojení dané aplikace společně s podrobnými informacemi si rozbalíte kliknutím na **>**.

Sloupce

Aplikace/Lokální IP – název aplikace, lokální IP adresy a porty, na kterých probíhá komunikace.

Vzdálená IP – IP adresa a port vzdáleného počítače.

Protokol – použitý transportní protokol.

Rychlost ven/Rychlost dovnitř – aktuální rychlost odchozích a příchozích dat.

Odesláno/Přijato – celkový objem přijatých a odeslaných dat.

Zobrazit/Skrýt detaily – pro zobrazení detailních informací je třeba kliknout na rozbalovací odkaz v dolní části okna.

Kliknutím pravým tlačítkem na aplikaci nebo IP adresu zobrazíte následující možnosti:

Překládat IP adresy na názvy počítačů – je-li to možné, síťové adresy se uvádějí ve formě názvu DNS, nikoli v číselné podobě IP adresy,

Zobrazovat pouze TCP spojení – Seznam zobrazuje spojení, která patří k protokolu TCP.

Zobrazit naslouchající spojení – po vybrání této možnosti se zobrazí pouze spojení, ve kterých neprobíhá

komunikace, ale port je v systému otevřený a čeká na spojení.

Zobrazit spojení v rámci počítače – tuto možnost vyberte, pokud chcete zobrazit pouze spojení, jejichž vzdáleným protějškem je lokální systém. Jedná se o spojení typu localhost.

Kliknutím pravým tlačítkem na spojení se zobrazí následující možnosti:

Zablokovat danou komunikaci – kliknutím ukončíte navázané spojení. Tato možnost je dostupná pouze nad aktivními spojeními.

Rychlost aktualizace – slouží pro nastavení intervalu, ve kterém se budou automaticky obnovovat informace o aktivních síťových spojeních.

Aktualizovat nyní – kliknutím aktualizujete obsah okna Síťová spojení.

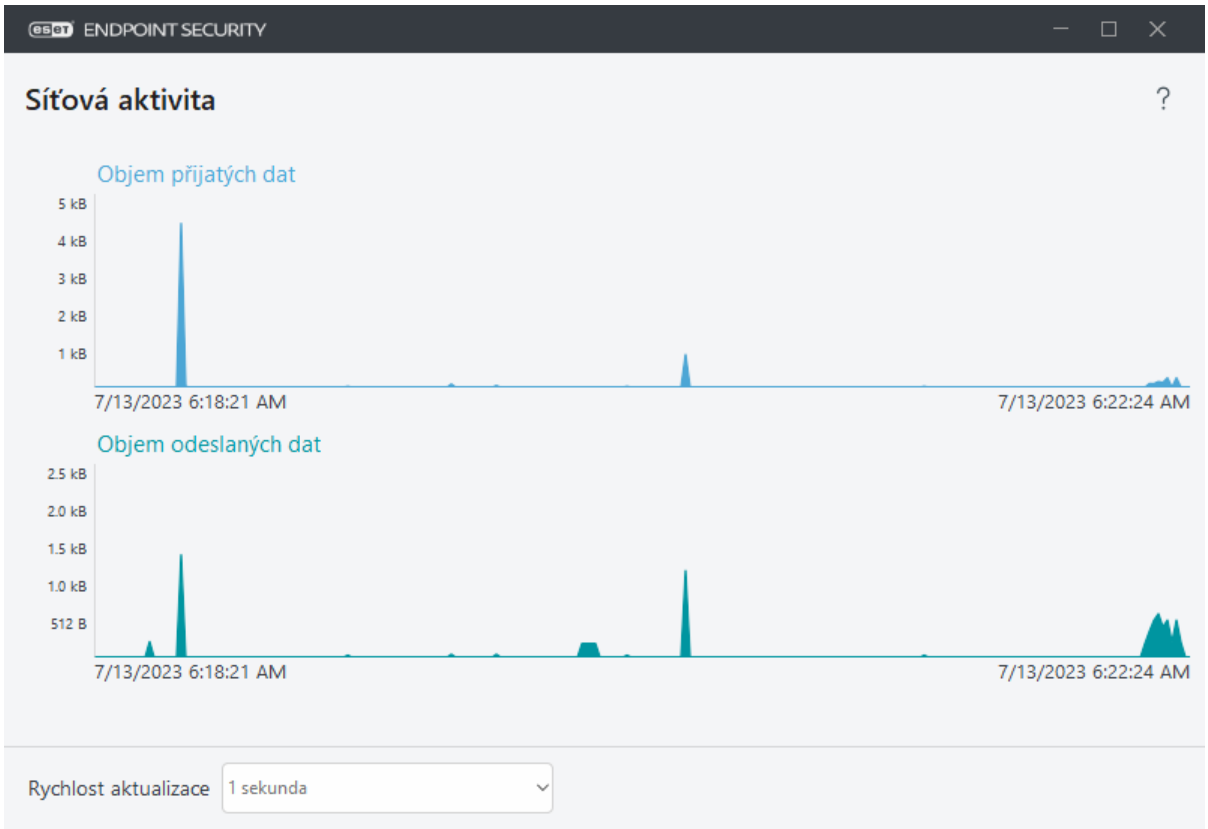
Následující volby jsou k dispozici pouze po kliknutí na aplikaci nebo proces, nikoli na aktivní spojení:

Dočasně zablokovat komunikaci pro daný proces – aktuální spojení aplikace bude zakázáno. Při vytvoření nového spojení se aplikuje předdefinované pravidlo firewallu. Popis nastavení naleznete v kapitole Pravidla firewallu.

Dočasně povolit komunikaci pro daný proces – aktuální spojení aplikace bude povoleno. Při vytvoření nového spojení se aplikuje předdefinované pravidlo firewallu. Popis nastavení naleznete v kapitole Pravidla firewallu.

Síťová aktivita

Pro zobrazení **Síťové aktivity** ve formě grafu klikněte na záložce **Nástroje** > **Síťová spojení** na ikonu grafu . Na základě vybrané rychlosti aktualizace se ve spodní části grafu zobrazuje časová osa, kde je zaznamenána síťová aktivita souborového systému v reálném čase. Ve spodní části se zobrazuje časová osa, jejíž měřítko můžete měnit pomocí rozbalovací nabídky **Rychlost aktualizace** v dolní části okna.



K dispozici jsou následující možnosti:

- **1 sekunda** – graf se obnoví každou sekundu a časová osa zobrazuje poslední čtyři minuty.
- **1 minuta (posledních 24 hodin)** – graf se obnoví každou minutu a časová osa zobrazuje posledních 24 hodin.
- **1 hodina (poslední měsíc)** – graf se obnoví každou hodinu a časová osa zobrazuje poslední měsíc.

Vertikální osa grafu probíhající aktivity souborového systému reprezentuje množství přijatých a odeslaných dat. Po najetí kurzorem myši do grafu se zobrazí přesné množství přijatých/odeslaných dat v konkrétní čas.

ESET SysInspector

ESET SysInspector je aplikace, která slouží k získání podrobných informací o systému zahrnující seznam nainstalovaných ovladačů a programů, síťových připojení a důležitých údajů z registru a hodnot závažnosti každé komponenty. Tyto informace mohou být užitečné při zjišťování příčiny podezřelého chování systému, nekompatibility software/hardware nebo infekci škodlivým kódem. Informace o používání ESET SysInspector naleznete v online nápovědě k ESET SysInspector.

V okně ESET SysInspector se nachází informace o vytvořených protokolech:

- **Čas** – čas vytvoření,
- **Komentář** – stručný komentář k vytvořenému záznamu,
- **Uživatel** – jméno uživatele, který vytvořil záznam,
- **Stav** – stav vytvoření.

Dostupné jsou následující akce:

- **Zobrazit** – po vybrání této možnosti si zobrazíte vybraný ESET SysInspector protokol. Případně klikněte pravým tlačítkem na požadovaný protokol a z kontextového menu vyberte možnost **Zobrazit**.
- **Vytvořit…** – kliknutím vytvoříte nový protokol. Vyčkejte na dokončení vytvoření protokolu ESET SysInspector (po dokončení se ve sloupci Stav zobrazí informace **Vytvořen**). Protokol se ukládá do C:\ProgramData\ESET\ESET Security\SysInspector.
- **Odstranit** – kliknutím odstraníte vybraný protokol ze seznamu.

Po kliknutí pravým tlačítkem myši na konkrétní protokol jsou kromě výše uvedených dostupné další možnosti:

- **Zobrazit** – po vybrání této možnosti si zobrazíte vybraný ESET SysInspector protokol (stejné jako dvojklik na vybraný protokol).
- **Vytvořit…** – kliknutím vytvoříte nový protokol. Vyčkejte na dokončení vytvoření protokolu ESET SysInspector (po dokončení se ve sloupci Stav zobrazí informace **Vytvořen**).
- **Odstranit** – kliknutím odstraníte vybraný protokol ze seznamu.
- **Odstranit vše** – vybráním této možnosti odstraníte všechny protokoly.
- **Exportovat** – po vybrání této možnosti uložíte protokol do .XML souboru nebo do zazipovaného .XML souboru.

Plánovač

spravuje a spouští naplánované úlohy s nastavenými parametry a vlastnostmi.

Plánovač je dostupný v hlavním okně programu ESET Endpoint Security na záložce **Nástroje** > **Plánovač**. **Plánovač** obsahuje seznam všech naplánovaných úloh a jejich nastavení jako je datum a čas provedení, použitý profil kontroly atp.

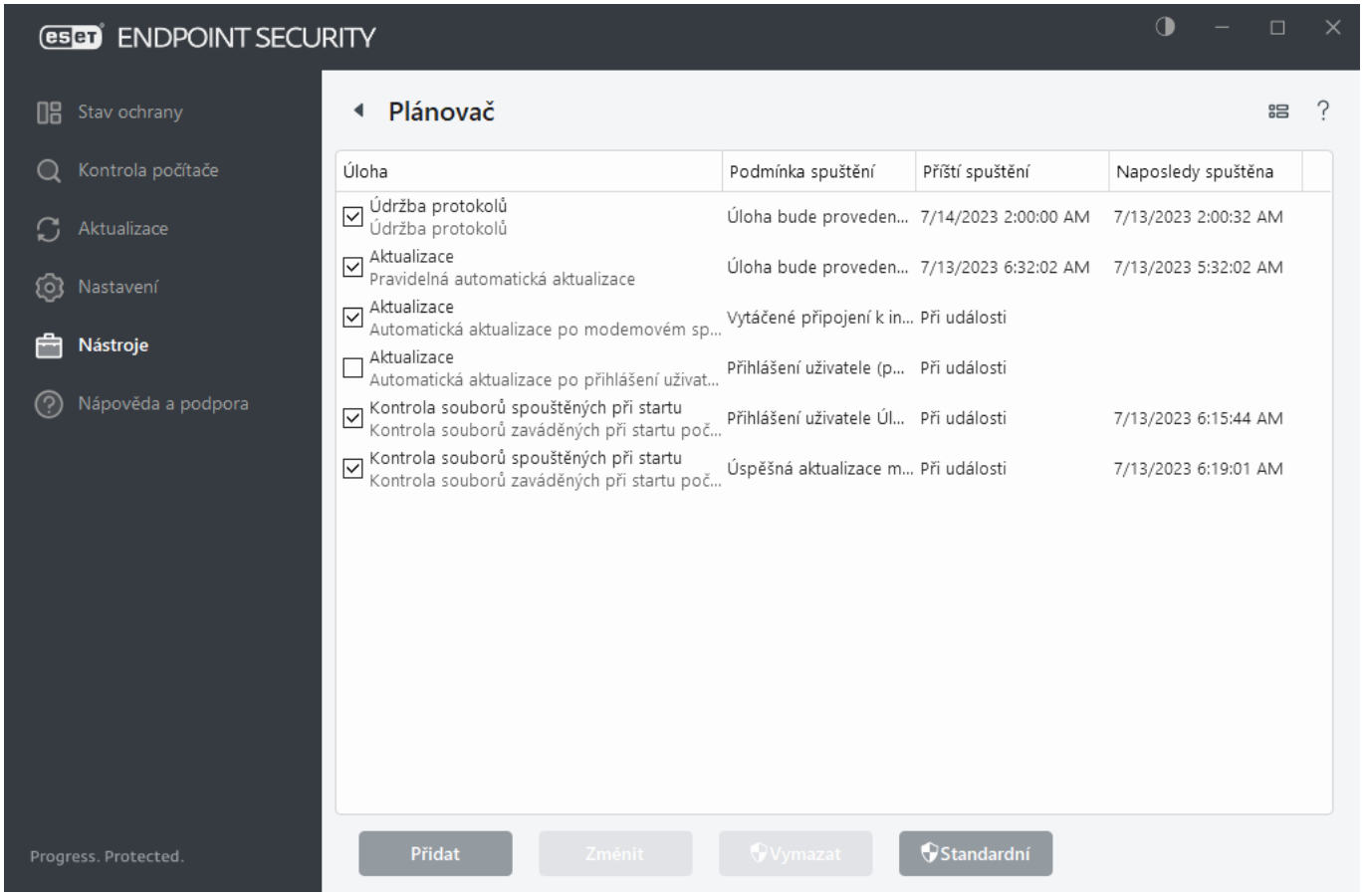
Plánovač slouží k plánování úloh jako je např. aktualizace programu, kontrola počítače, kontrola souborů spouštěných po startu nebo pravidelná údržba protokolů. Přímo v hlavním okně Plánovače můžete pomocí tlačítek **Přidat** a **Odstranit** úlohy vytvářet nebo mazat. Po kliknutí pravým tlačítkem myši na konkrétní položku v Plánovači se zobrazí kontextové menu s nabídkou možných akcí: zobrazení detailů o úloze, okamžité provedení úlohy, přidání nové úlohy, změnu, případně odstranění již existující úlohy. Pomocí zaškrtávacích polí můžete (de)aktivovat provádění jednotlivých úloh.

Standardně **Plánovač** zobrazuje následující naplánované úlohy:

- **Údržba protokolů**,
- **Pravidelná automatická aktualizace**,
- **Automatická aktualizace po modemovém spojení**,
- **Automatická aktualizace po přihlášení uživatele**,
- **Kontrola souborů spouštěných při startu** (při přihlášení uživatele na počítač),
- **Kontrola souborů spouštěných po startu** (po úspěšné aktualizaci modulů),

> Prostřednictvím ESET PROTECT můžete spouštěním naplánovaných úloh v náhodném čase snížit zatížení sítě, což oceníte především ve velkých sítích. Pomocí této možnosti můžete definovat časové období, ve kterém má být úloha spuštěna na všech v počítačích v síti. Při spuštění úlohy se vygeneruje unikátní čas pro každou stanici v síti tak, aby se úloha na klientských stanicích spustila v náhodném čase. To zabrání přetížení serveru a podobným problémům (například některé servery mohou hlásit DoS útok při provádění hromadné aktualizace na všech stanicích v síti ve stejný čas).

Pro úpravu existujících (a to jak předdefinovaných, tak vlastních) úloh použijte kontextové menu, ve kterém vyberte možnost **Změnit**, případně po vybrání požadované úlohy klikněte na tlačítko **Změnit**.



Přidání nové úlohy

1. Klikněte na tlačítko **Přidat** ve spodní části okna.
2. Zadejte název úlohy.
3. Z rozbalovacího menu vyberte požadovaný typ úlohy:

- **Spuštění externí aplikace** – vyberte si aplikaci, kterou chcete pomocí plánovače spustit.
- **Údržba protokolů** – v protokolech mohou přirozeně zůstat zbytky po již smazaných záznamech. Tato úloha zajistí optimalizaci záznamů v protokolech, což zajistí efektivnější a rychlejší práci s nimi.
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému.
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě.
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači,
- **Aktualizace** – zajišťuje aktualizaci detekčního jádra a programových modulů.

4. Pro aktivování úlohy přepněte přepínač do polohy **Zapnuto** (to můžete udělat kdykoli později přímo v seznamu naplánovaných úloh pomocí zaškrtávacího pole) a po kliknutí na tlačítko **Další** vyberte interval opakování:

- **Jednou** – úloha se provede pouze jednou v naplánovaném čase.
- **Opakovaně** – úloha se bude provádět opakovaně každých x minut.
- **Denně** – úloha se provede každý den ve stanový čas.
- **Týdně** – úloha se bude provádět v určitý den/dny v týdnu ve stanoveném čase.
- **Při události** – úloha se provede při určité situaci.

5. Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii nebo počítače z UPS, zapněte možnost **Nespouštět úlohu, pokud je počítač napájen z baterie**. Po kliknutí na tlačítko Další

zadejte čas **Provedení úlohy**. Pokud nebude možné úlohu v daném čase spustit, nastavte alternativní termín pro spuštění úlohy:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

Informace o naplánované úloze si můžete kdykoli zobrazit po kliknutí pravým tlačítkem myši na úlohu a vybrání možnosti **Zobrazit detaily úlohy**.

Možnosti naplánované kontroly

V tomto dialogovém okně můžete konfigurovat detaily naplánované úlohy kontroly počítače.

V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, klikněte na **Rozšířená nastavení** a následně vyberte možnost **Neléčit**. Historie kontrol je zaznamenána do protokolu kontrol.

Vybráním možnosti **Ignorovat výjimky** nebudou brány v potaz výjimky a dané soubory se zkontrolují.

Z rozbalovacího menu můžete vybrat akci, která se má provést po dokončení kontroly:

- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.
- **Vypnout** – počítač se po dokončení kontroly vypne,
- **Restartovat** – počítač se po dokončení kontroly restartuje,
- **Restartovat, pokud je potřeba** – počítač se po dokončení kontroly restartuje, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Vynutit restart** – po dokončení kontroly dojde k automatickému zavření všech otevřených aplikací a počítač se restartuje.
- **V případě potřeby vynutit restart** – po dokončení kontroly se vynutí restartování počítače, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Režim spánku** – aktuální relace se uloží do operační paměti a počítač přejde do úsporného stavu. Následné probuzení počítače je rychlé a můžete ihned pokračovat v rozdělené činnosti.
- **Hibernovat** – uloží aktuální relaci na pevný disk a počítač se kompletně vypne. Při další spuštění počítače se obnoví poslední stav.

> Akce **Režim spánku** nebo **Hibernace** je dostupná na základě Nastavení napájení a režimu spánku, případně možnostech vašeho zařízení. Mějte na paměti, že uspaný počítač je pouze v režimu spánku a stále běží. Stále je napájen ze sítě, případně z baterie. Pro maximální výdrž baterie doporučujeme vybrat možnost Hibernovat.

Možnost **Kontrolu nemůže uživatel přerušit** vyberte v případě, kdy chcete ne-privilegovanému uživateli zabránit v přerušení definované akce.

Parametr **Uživatel může pozastavit kontrolu o max. (min)** použijte, pokud chcete umožnit odložení kontroly počítače na později – o určitou dobu.

Další informace naleznete v kapitole Průběh kontroly.

Informace o naplánované úloze

Toto okno zobrazuje detailní a přehledné informace o vybrané úloze. Informace získáte dvojklikem na danou úlohu v Plánovači (Nástroje > (Další nástroje) > Plánovač) nebo kliknutím pravým tlačítkem na úlohu tamtéž a ze zobrazeného kontextového menu vybráním možnosti **Zobrazit detaily úlohy**.

Detaily úlohy

Zadejte **název úlohy**, vyberte její **typ** a pokračujte kliknutím na tlačítko **Další**:

- **Spuštění externí aplikace** – vyberte si aplikaci, kterou chcete pomocí plánovače spustit.
- **Údržba protokolů** – v protokolech mohou přirozeně zůstat zbytky po již smazaných záznamech. Tato úloha zajistí optimalizaci záznamů v protokolech, což zajistí efektivnější a rychlejší práci s nimi.
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému.
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě.
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači,
- **Aktualizace** – zajišťuje aktualizaci detekčních a programových modulů.

Provedení úlohy

Úloha se bude provádět opakovaně ve vybraném časovém intervalu. Prosím, vyberte jednu z možností:

- **Jednou** – úloha se provede pouze jednou v naplánovaném čase,
- **Opakovaně** – úloha se provede opakovaně každých x hodin,
- **Denně** – úloha bude provedena každý den ve stanovený čas,
- **Týdně** – úloha bude provedena v určitý den v týdnu ve stanovený čas,
- **Při události** – úloha bude provedena po určité události.

Nespouštět úlohu, pokud je počítač napájen z baterie – pokud je v době plánovaného spuštění úlohy počítač napájen z baterie, nebude úloha provedena. To platí i v případě napájení z UPS.

Provedení úlohy – Jednou

Provedení úlohy – úloha bude provedena jednou ve stanovený datum a čas.

Provedení úlohy – Denně

Úloha bude provedena každý den ve stanovený čas.

Provedení úlohy – Týdně

Úloha bude provedena v určitý den v týdnu ve stanovený čas.

Provedení úlohy – Při události

Úloha bude provedena při jedné z následujících událostí:

- **Při každém startu počítače**,
- **Při prvním startu počítače během dne**,
- **Při modemovém připojení na internet/připojení do VPN**,
- **Při úspěšné aktualizaci modulů**,
- **Při úspěšné aktualizaci programu**,
- **Při přihlášení uživatele na počítač**,
- **Při detekci hrozby**.

Pokud plánujete provedení úlohy při události, můžete definovat minimální interval mezi dvěma provedeními úlohy. Například, pokud se přihlašujete na počítač vícekrát za den, nastavením intervalu provedení na 24 hodin se tato úloha spustí pouze při prvním přihlášení a poté až následující den.

Neprovedení úlohy

Úloha může být přeskočena v případě, kdy je počítač napájen z baterie, nebo je vypnutý. Vyberte akci, jak se má program v takovém případě zachovat, a pokračujte kliknutím na tlačítko **Další**:

- **Při dalším naplánovaném termínu** – úloha bude provedena v dalším naplánovaném termínu.
- **Jakmile to bude možné** – úloha bude provedena po spuštění počítače.
- **Okamžitě, pokud doba od posledního spuštění překročí (v hodinách)** – jedná se o časové období, které uplyne od doby, kdy měla být úloha spuštěna poprvé. Pokud dojde k překročení této doby, úloha se okamžitě spustí.

Příklady úlohy s podmínkou "Okamžitě, pokud od posledního provedení uplynul stanovený interval (v hodinách)"

V příkladu je úloha nastavena tak, aby se spouštěla opakovaně každou hodinu. V poli **Okamžitě, pokud od posledního provedení uplynul stanovený interval (v hodinách)** je nastavena hodnota 2 hodiny. Úloha se spustí ve 13:00 a po dokončení počítač přejde do režimu spánku:
• Počítač se probudí v 15:30. K prvnímu vynechanému spuštění úlohy došlo ve 14:00. Od 14:00 uplynulo pouze 1,5 hodiny, takže úloha bude spuštěna v 16:00.
• Počítač se probudí v 16:30. K prvnímu vynechanému spuštění úlohy došlo ve 14:00. Od 14:00 uplynuly 2,5 hodiny, takže se úloha spustí okamžitě.

Detaily úlohy – Aktualizace

Chcete-li program aktualizovat ze dvou aktualizačních serverů, je nutné vytvořit dva různé profily aktualizace. Pokud se vám nepodaří stáhnout aktualizační soubory, program se automaticky přepne na alternativní. Tuto možnost můžete použít například pro notebooky, které jsou aktualizovány z lokálních LAN aktualizačních serverů a zároveň jsou uživatelé často přistupují k internetu. V případě neúspěšné aktualizace z hlavního profilu s

nastavením pro lokální LAN, se aktualizace provede pomocí alternativního profilu nastaveného pro aktualizaci přímo ze serverů společnosti ESET.

Detaily úlohy – Spuštění aplikace

Pomocí tohoto typu úlohy si můžete naplánovat spuštění externí aplikace.

Spustitelný soubor – vyberte soubor kliknutím na **…** nebo zadejte cestu k souboru ručně.

Pracovní složka – definuje pracovní složku externí aplikace. Všechny dočasné soubory související se **spustitelným souborem** budou vytvořeny v této složce.

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Kliknutím na tlačítko **Dokončit** potvrdíte její naplánování.

Odeslání vzorku k analýze

V případě, že máte soubor s podezřelým chováním nebo jste narazili na internetu na infikovanou stránku, můžete tato data odeslat na analýzu do virové laboratoře ESET (nemusí být k dispozici v závislosti na konfiguraci ESET LiveGrid®).

Vzorky zasílejte pouze v případě, kdy splňuje jedno z následujících kritérií:
• Soubor není produktem ESET detekován
• Vzorek je detekován nesprávně jako hrozba
• Mějte na paměti, že osobní soubory nepřijímáme jako vzorky (neprovádíme jejich kontrolu za uživatele)
• Nezapomeňte vyplnit předmět a přiložte maximální možné množství informací o daném vzorku (jak jste se k němu dostali, od koho jste odkaz na ní obdrželi, screenshot apod.)

Vzorek k analýze (soubor nebo stránku) můžete do společnosti zaslat jedním z níže uvedených způsobů:

1. Prostřednictvím dialogového okna, které naleznete v hlavním okně produktu na záložce **Nástroje** > **Odeslat soubor k analýze**.
2. Případně můžete soubor zaslat e-mailem. Pokud dáváte přednost této možnosti, prosím dbejte na to, abyste soubor přidali do archivu WinRAR/ZIP a ochránili archiv heslem "infected" předtím, než jej odešlete na adresu samples@eset.com.
3. Jak nahlásit spam, falešnou detekci spamu nebo špatně kategorizované webové stránky funkcí Filtrování obsahu webu se dozvíte v článku z naší Databáze znalostí.

V zobrazeném dialogovém **okně pro odeslání vzorku** vyberte z rozbalovacího menu **Důvod odeslání vzorku** možnost, která nejlépe vystihuje danou situaci:

- Podezřelý soubor
- Podezřelá stránka (webová stránka infikovaná škodlivým kódem)
- Falešně detekovaný soubor (soubor detekovaný jako infikovaný není infikovaný)
- Falešně detekovaná stránka
- Ostatní

Soubor/Stránka – cesta k souboru nebo URL adresa.

Kontaktní e-mail – na tento e-mail vás budou pracovníci virové laboratoře ESET kontaktovat, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné. V takovém případě vyberte možnost **Odeslat anonymně**.

> Na zadanou e-mailovou adresu vás budou pracovníci virové laboratoře ESET kontaktovat pouze v případě, kdy budou potřebovat více informací. Denně do společnosti ESET chodí několik desítek tisíc souborů, a není možné na každý e-mail reagovat.
> Pokud se ukáže, že se jedná o nebezpečnou aplikaci nebo webovou stránku, její detekce bude přidána v některé z nejbližších aktualizací.

Podezřelý soubor

Pozorované projevy a příznaky infekce – uveďte prosím, co nejdetailnější popis chování souboru v systému pro přesnější analýzu souboru.

Původ souboru (URL adresa nebo výrobce aplikace) – uveďte URL adresu, případně jeho výrobce (pokud je znám) pro lepší identifikaci souboru.

Poznámky a doplňující informace – veškeré další informace, které by mohly pomoci při identifikaci a zpracování souboru.

> Pouze první parametr – **Pozorované projevy a příznaky infekce** – je povinný, ale poskytnutím doplňujících informací pomůžete významnou měrou při identifikaci a zpracování vzorků.

Podezřelá stránka

Vyberte z rozbalovacího menu **Co je špatného na této stránce** odpovídající možnost:

- **Infikovaná** – webová stránka obsahuje viry nebo jiný škodlivý kód,
- **Phishing** – často využíván pro získání citlivých dat, jako jsou čísla bankovních účtů, PIN kódy a další. Více o tomto typu útoku se můžete dočíst ve slovníku pojmů.
- **Scam** – podvodné webové stránky vytvořené za účelem rychlého zisku,
- Vyberte možnost **Ostatní**, pokud žádná z výše uvedených neodpovídá obsahu stránky.

Poznámky a doplňující informace – zadáním dalších informací a popisu pomůžete při analyzování podezřelé stránky.

Falešně detekovaný soubor

Prosíme vás, abyste nám zasílali soubory, které byly detekovány jako škodlivé, ale ve skutečnosti nejsou. Falešný poplach (False positive, zkráceně FP) může nastat, když struktury souboru mají stejné charakteristiky jako vzorky obsažené v detekčním jádru.

Název a verze aplikace – název a verze aplikace pro identifikaci aplikace.

Původ souboru (URL adresa nebo výrobce aplikace) – zadejte původ souboru (zdroj) a jakým způsobem jste k souboru přišli.

Účel aplikace – charakterizujte účel a typ aplikace (např. prohlížeč, přehrávač médií atd.) pro rychlejší zařazení a

identifikaci.

Poznámky a doplňující informace – zadáním dalších informací a popisu pomůžete při analyzování podezřelého souboru.

> První tři parametry jsou povinné z důvodu lepší identifikace legitimní aplikace. Poskytnutím doplňujících informací pomůžete významnou měrou při identifikaci a zpracování vzorků.

Falešně detekovaná stránka

Při odesílání stránky, která je falešně detekována jako infikovaná, scam nebo phishing, ale ve skutečnosti není, vyžadujeme zadání dalších informací. Falešný poplach (False positive, zkráceně FP) může nastat, když struktury souboru mají stejné charakteristiky jako vzorky obsažené v detekčním jádru. Poskytnutím těchto informací pomůžete vylepšit antivirové a anti-phishingové jádro.

Poznámky a doplňující informace – zadáním dalších informací a popisu pomůžete při analyzování podezřelé webové stránky.

Ostatní

Tento formulář použijte v případě, že soubor nevyhovuje definici **Podezřelý soubor** nebo **Falešný poplach.**

Důvod odesílání souboru – uveďte prosím důvod odeslání souboru a co nejpřesnější popis souboru.

Karanténa

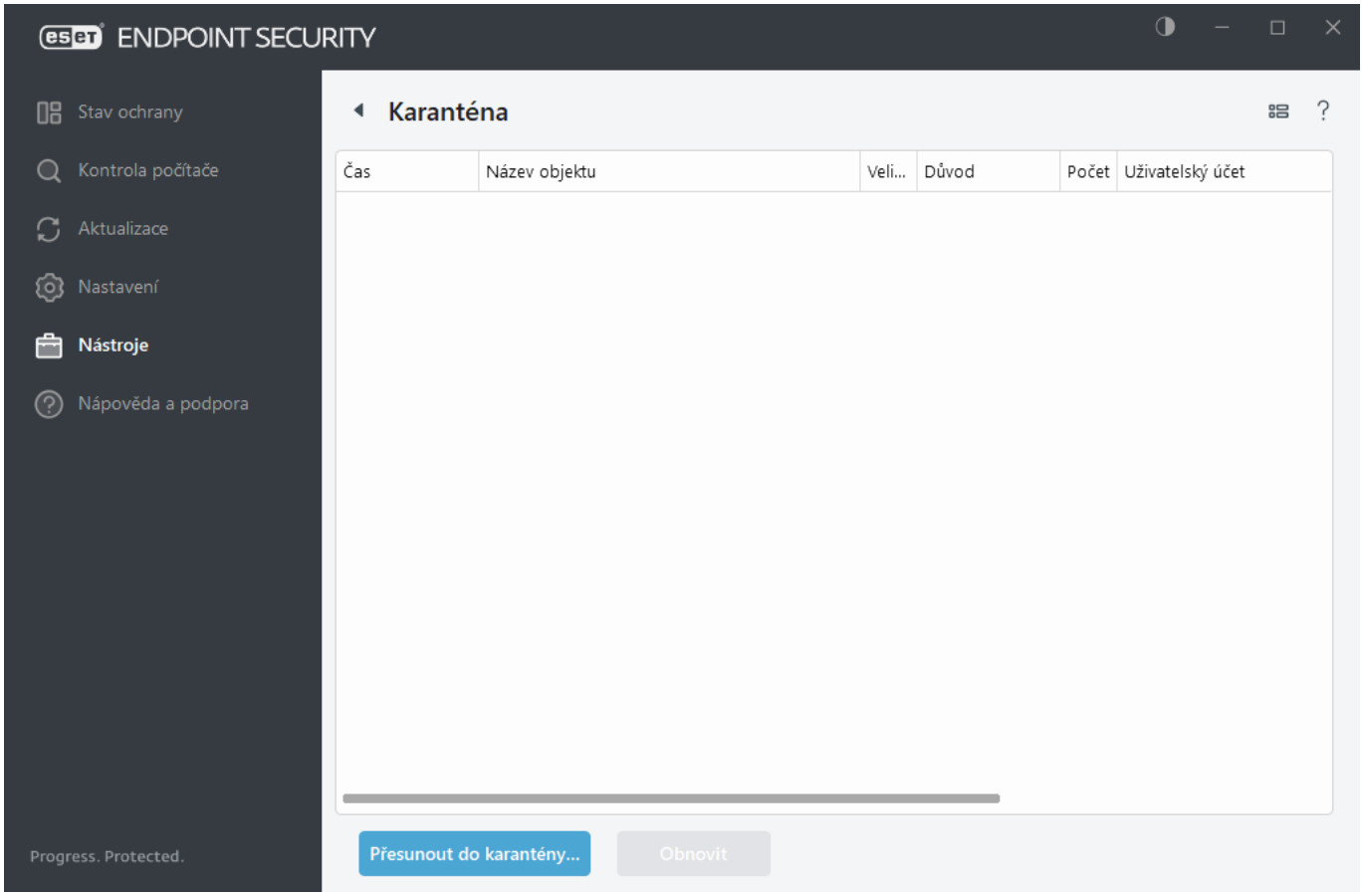
Hlavní funkcí karantény je bezpečně uschovat nahlášené objekty (jako je malware, infikované soubory nebo potenciálně nechtěné aplikace).

Karanténa je dostupná v hlavním okně programu ESET Endpoint Security na záložce **Nástroje** > **Karanténa**.

Soubory uložené v karanténě si můžete prohlédnout v přehledné tabulce včetně informací o:

- datu a čase přidání souboru do karantény,
- cesty k původnímu umístění souboru,
- jeho velikosti v bajtech,
- důvodu proč byl přidán do karantény (např. objekt přidaný uživatelem),
- a počtu detekcí. (např. duplikovanou detekcí stejného souboru, nebo pokud se jedná o archiv obsahující více infiltrací).

Vzdálená správa karantény na klientovi



Vložení objektu do karantény

ESET Endpoint Security automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nezrušili v okně s upozorněním).

Soubory mohou být umístěny do karantény, pokud:

- nemohou být léčeny,
- pokud není bezpečné a doporučené jejich odstranění,
- pokud byly ESET Endpoint Security falešně detekovány,
- nebo pokud soubor vykazuje podezřelou aktivitu, ale není detekován skenerem.

Pro uložení souboru do karantény máte několik možností:

- přetáhněte ji způsobem Drag and drop (nakliknout na soubor levým tlačítkem myši, podržet levé tlačítko, přesunout do zvýrazněné oblasti a tlačítko pustit). Po přesunutí souboru se okno aplikace přesune do popředí.
- Klikněte na **Přidat do karantény** z hlavního okna programu.
- Využít můžete rovněž kontextové menu – klikněte pravým tlačítkem v okně **Karantény** a vyberte možnost **Přesunout do karantény…**.

Obnovení z karantény

Soubory v karanténě lze vrátit do původního umístění:

- K tomuto účelu použijte funkci **Obnovit**, která je k dispozici v místní nabídce kliknutím pravým tlačítkem myši na daný soubor v karanténě.

- Pokud je soubor označen jako potenciálně nechtěná aplikace, je povolena možnost **Obnovit a vyloučit z kontroly**. Viz také kapitolu Výjimky.
- V kontextovém menu se dále nachází možnost **Obnovit do…**, pomocí které můžete obnovit soubor na jiné místo než to, ze kterého byl původně smazán.
- Funkce obnovení není dostupná například pro soubory umístěné ve sdílené síťové složce pro čtení.

Odstranění z karantény

Klikněte pravým tlačítkem na objekt v karanténě a vyberte možnost **Odstranit z karantény**, případně vyberte objekt a stiskněte na klávesnici klávesu **Delete**. Rovněž můžete vybrat více položek a smazat je najednou. Smazané objekty budou trvale odstraněny z karantény a vašeho počítače.

Odeslání souboru z karantény k analýze

Pokud máte v karanténě uložen soubor s podezřelým chováním, nebo byl soubor označen jako infikovaný nesprávně (např. heuristickou analýzou kódu), můžete vzorek odeslat do společnosti ESET k analýze. Vyberte daný soubor, klikněte na něj pravým tlačítkem myši a z kontextového menu vyberte možnost **Odeslat k analýze**.

Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
- Správa karantény v ESET PROTECT
- Program ESET mě upozornil na detekci. Co mám dělat?

Nápověda a podpora

Kliknutím na položku **Nápověda a podpora** v hlavním okně programu zobrazíte informace o podpoře a nástroje pro řešení problémů, které vám pomohou vyřešit problémy, s nimiž se můžete setkat.

Nainstalovaný produkt

- O programu ESET Endpoint Security – kliknutím si zobrazíte souhrnné informace o vámi nainstalovaném programu ESET Endpoint Security.
- Průvodce řešením problémů s produktem – po kliknutí si zobrazíte návody pro odstranění nejčastějších problémů.
- Průvodce řešením problémů s licencí – po kliknutí si zobrazíte nejčastější problémy týkající se aktivace nebo změny licence společně s jejich řešením.
- Změnit licenci – po kliknutí se zobrazí dialogové okno, pomocí kterého můžete produkt aktivovat.

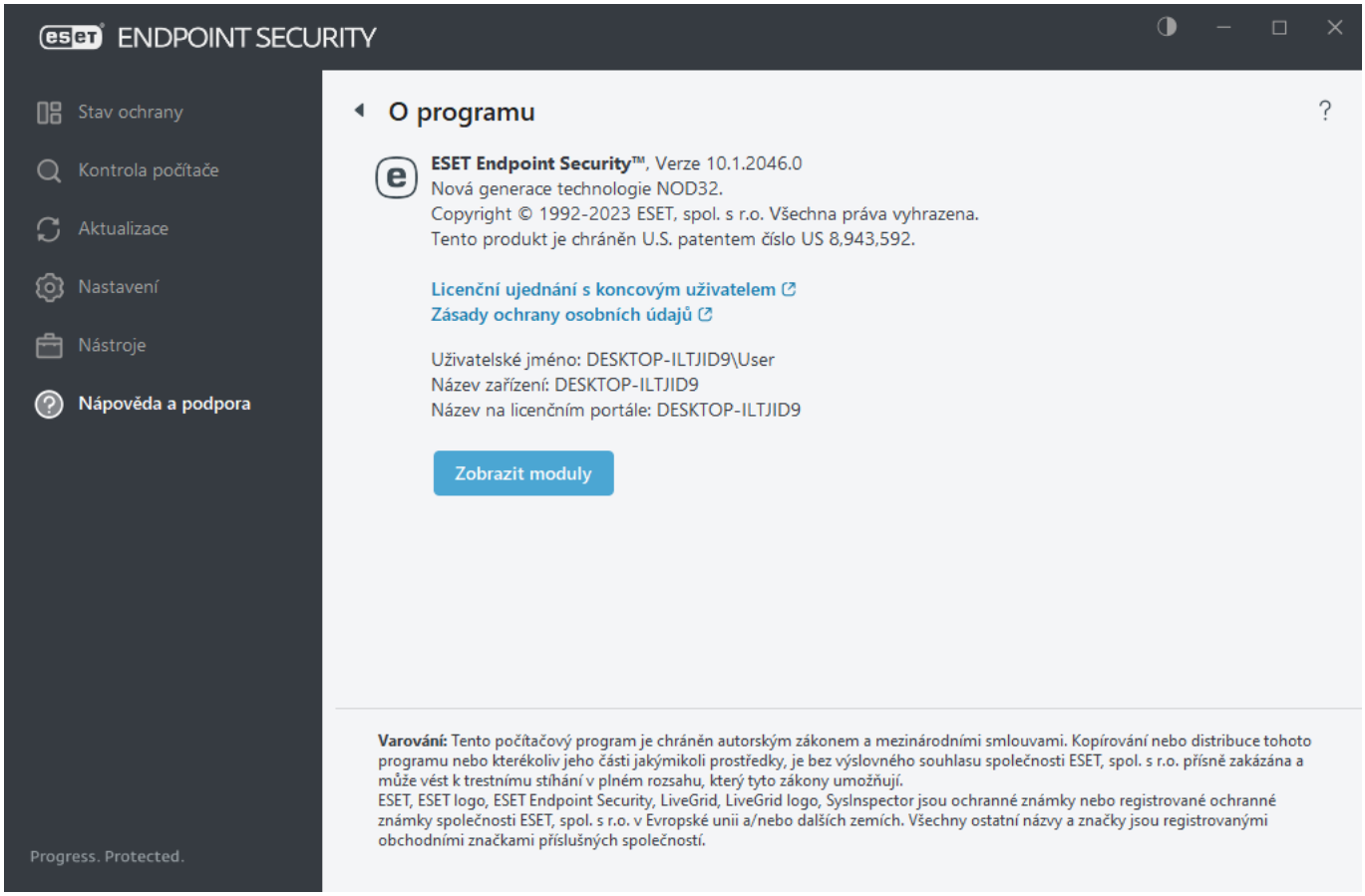
Otevřít nápovědu – kliknutím na odkaz si zobrazíte nápovědu k programu ESET Endpoint Security.

Technická podpora

Databáze znalostí – internetová ESET Databáze znalostí obsahuje odpovědi na často kladené otázky a doporučené způsoby pro řešení problémů. Pravidelná aktualizace z ní dělá nejrychlejší nástroj k řešení mnoha typů problémů.

O programu ESET Endpoint Security

Toto okno zobrazuje informace o verzi ESET Endpoint Security a o vašem počítači.



Pro zobrazení seznamu používaných programových modulů včetně jejich verzí klikněte na tlačítko **Zobrazit moduly**.

- Informace o modulech můžete zkopírovat do schránky kliknutím na **Kopírovat**. To se hodí v případě, že kontaktujete technickou podporou společnosti ESET z důvodu řešení technického problému.
- Pokud kliknete na položku **Detekční jádro** v okně Modulů, otevře se ESET Virus radar, který obsahuje informace o každé verzi Detekčního jádra ESET.

Odeslat konfiguraci systému

Aby mohli specialisté technické podpory rychle a relevantně reagovat na dotazy zákazníků, vyžadují zaslání konfigurace produktu ESET Endpoint Security, detailních informací o systému včetně spuštěných procesů a záznamů v registru – tedy protokolu z nástroje ESET SysInspector. Společnost ESET použije tyto údaje pouze pro poskytnutí technické pomoci zákazníkovi.

Po odeslání webového formuláře *** se do společnosti ESET odešlou informace o konfiguraci vašeho systému. Mějte na paměti, že specialisté technické podpory vás v tomto případě mohou následně požádat o dodatečné zaslání těchto dat. Odeslání webového formuláře bez jakýchkoli dat, proveďte kliknutím na **Neodesílat data** a pokračujte.

Odesílání údajů o konfiguraci systému můžete nastavit v Rozšířeném nastavení > **Nástroje** > **Diagnostika** > Technická podpora.

Pokud jste se rozhodli odeslat údaje o konfiguraci systému, je nutné vyplnit a odeslat webový formulář. V opačném případě nebude tiket vytvořen a údaje o konfiguraci systému se ztratí. Pokud údaje o konfiguraci systému nelze odeslat, vyplňte webový formulář a vyčkejte na pokyny technické podpory.

Technická podpora

V hlavním okně programu přejděte na záložku **Nápověda a podpora**, klikněte na **Technická podpora**.

Kontaktovat Technickou podporu

Požádat o podporu – v případě, že nenajdete řešení problému, můžete kontaktovat naše specialisty technické podpory prostřednictvím formuláře na webových stránkách společnosti ESET. V závislosti na konfiguraci produktu se před vyplněním webového formuláře může zobrazit dialogové okno Odeslat konfiguraci systému.

Získání informací pro technickou podporu

Základní informace pro technickou podporu – tuto možnost použijte, pokud po vás specialisté technické podpory vyžadují informace o vašem počítači (informace o licenci, verzi produktu, operačním systému, atp.)

ESET Log Collector – po kliknutí budete přesměrováni do Databáze znalostí společnosti ESET pro stažení diagnostického nástroje. ESET Log Collector automaticky sesbírá protokoly a informace o systému, které specialistům technické podpory usnadní diagnostiku problému a urychlí přípravu řešení. Pro více informací přejděte do online uživatelské příručky k ESET Log Collector.

Pro vytvoření rozšířených protokolů s informacemi, které pomohou vývojářům s diagnostikou problému, klikněte na možnost **Rozšířené protokolování**. Úroveň protokolování je v tomto případě nastavena na hodnotu **Diagnostické**. Rozšířené protokolování se automaticky deaktivuje po dvou hodinách, případně tento režim můžete ručně ukončit kliknutím na **Zastavit rozšířené protokolování**. Po vytvoření všech protokolů se zobrazí informační okno v němž naleznete odkaz pro zobrazení složky s diagnostickými protokoly.

Rozšířená nastavení

Rozšířená nastavení umožňují podrobné nastavení ESET Endpoint Security podle vašich potřeb.

Chcete-li otevřít Rozšířená nastavení, otevřete hlavní okno programu a stiskněte klávesu **F5** na klávesnici nebo klikněte na **Nastavení** > **Rozšířená nastavení**.

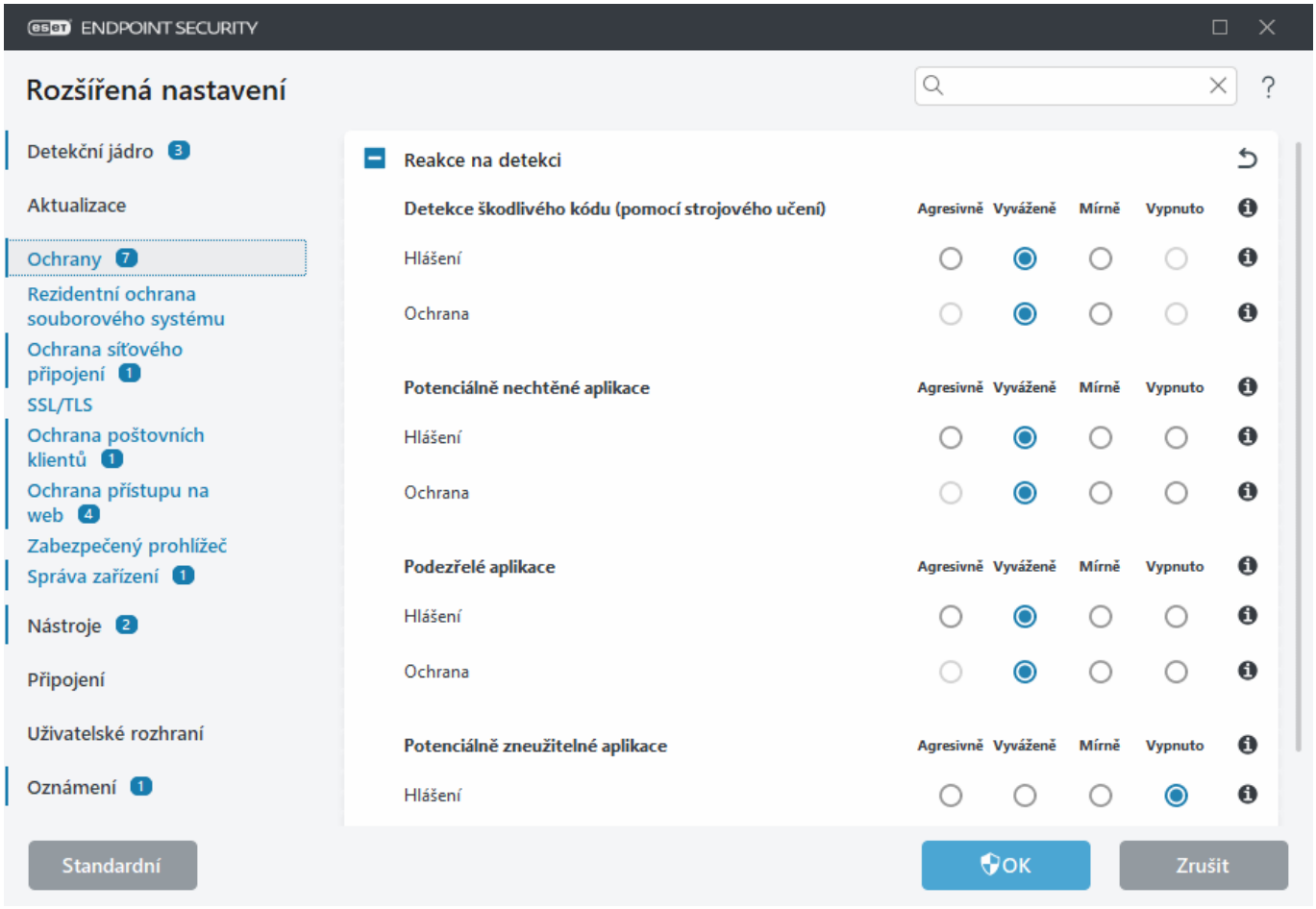
Při vytváření politiky v ESET PROTECT Web Console můžete u každého nastavení definovat příznak. Nastavení s příznakem má prioritu a nemůže být přepsáno pozdější politikou (pouze pokud obsahuje poslední politika příznak). To zajišťuje, aby nastavení nebylo změněno (např. uživatelem nebo pozdější politikou během slučování). Pro více informací o příznacích se podívejte do online nápovědy k ESET PROTECT.

V závislosti na Přístupu k nastavení můžete být vyzváni k zadání hesla pro otevření Rozšířeného nastavení.

V rozšířeném nastavení můžete provádět následující nastavení:

- Detekční jádro
- Aktualizace

- Ochrany
- Nástroje
- Připojení
- Uživatelské rozhraní
- Oznámení



Detekční jádro

Rozšířená nastavení > **Detekční jádro** umožňuje konfigurovat následující možnosti:

- Výjimky
- Rozšířená nastavení
- Kontrola síťové komunikace

Výjimky

Vytvořením **výjimky** zabráníte tomu, aby detekční jádro kontrolovalo vámi požadovaný objekt. Pro zajištění kontroly všech objektů na výskyt hrozeb doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Příkladem, kdy je nutné vyloučit objekt z kontroly (například velké databázové soubory), je situace, kdy v průběhu kontroly dochází ke zpomalení počítače nebo konfliktu s právě používanou aplikací.

Prostřednictvím výkonnostních výjimek můžete vyloučit soubory nebo složky z kontroly. Výkonnostní výjimky je vhodné využít v případě, kdy chcete z kontroly vyloučit aplikace na úrovni konkrétních souborů z důvodu, že jejich kontrola způsobuje nezvyklé chování systému, případně snižuje výkon.

Prostřednictvím detekčních výjimek můžete vyloučit objekty z léčení na základě názvu detekce, cesty nebo kontrolního součtu. Detekční výjimky se nechovají stejně jako Výkonnostní výjimky, které slouží k vyloučení souborů nebo složek z kontroly. Objekt se vyloučí v případě, že je zachycen detekčním jádrem a vyhovuje některému z pravidel uvedených na seznamu detekčních výjimek.

Nezaměňujte mezi sebou jednotlivé typy výjimek:

- Vyloučené procesy – z kontroly budou vyloučeny všechny souborové operace prováděné danou aplikací (to může být užitečné pro zvýšení rychlosti zálohování a dostupnosti služeb).
- Vyloučené přípony souborů
- HIPS výjimky
- Filtr výjimek pro cloudovou ochranu

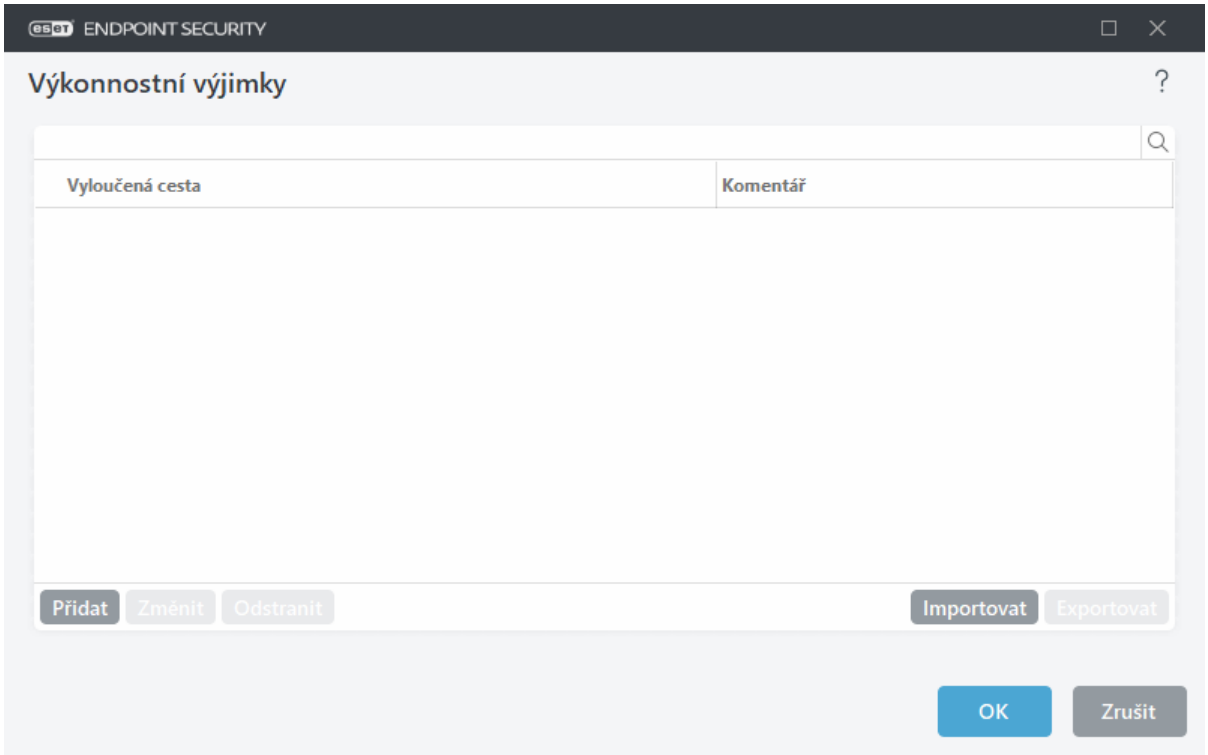
Výkonnostní výjimky

Prostřednictvím výkonnostních výjimek můžete vyloučit soubory nebo složky z kontroly.

Pro zajištění kontroly všech objektů na výskyt hrozeb doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Příkladem, kdy je nutné vyloučit objekt z kontroly (například velké databázové soubory), je situace, kdy v průběhu kontroly dochází ke zpomalení počítače nebo konfliktu s právě používanou aplikací.

Seznam souborů a složek vyloučených z kontroly můžete definovat v Rozšířených nastaveních > **Detekční jádro** > **Výjimky** > **Výkonnostní výjimky** > **Změnit**.

Pro vyloučení objektu z kontroly klikněte na tlačítko **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury.



Pokud soubor vyhovuje definované výjimce, nebude v něm detekovat hrozby **Rezidentní ochrana souborového systému**, ani naplánovaná či ručně spuštěná **Kontrola počítače**.

Ovládací prvky

- **Přidat** – kliknutím přidáte nový záznam na seznam objektů vyloučených z kontroly.
- **Změnit** – kliknutím upravíte vybraný záznam.
- **Odstranit** – odstraní vybranou položku (CTRL + klik pro výběr více položek).
- **Import** / **Export** – importování a exportování výkonnostních výjimek je užitečné například pokud si potřebujete zálohovat stávající seznam výjimek, a chcete se k němu později vrátit. Export nastavení oceníte také v případě nespravovaných prostředí, kdy pro zajištění stejné konfigurace na více počítačích postačí pouze naimportovat daný .txt soubor.

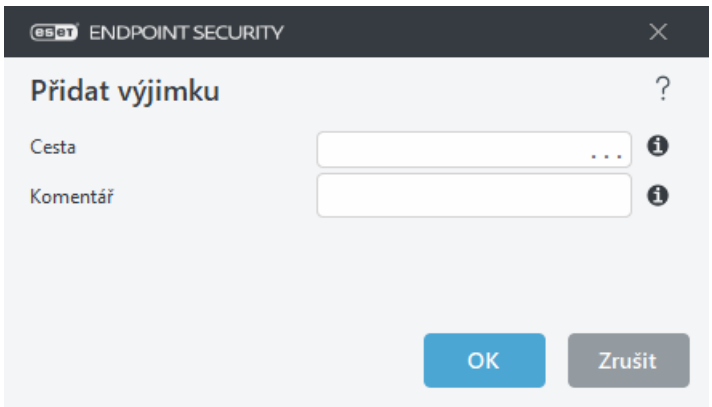
  Zobrazit příklad formátu souboru

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagem
ent.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

Přidání a úprava výkonnostních výjimek

V tomto dialogovém okně můžete vyloučit (soubor nebo složku) z kontroly v tomto počítači.

Pro vybrání cesty klikněte na symbol **…** v poli **Cesta**.
Pokud budete cestu zadávat ručně, podívejte se na níže uvedené příklady výjimek.



Pro vyloučení skupiny souborů z kontroly můžete použít zástupné znaky. Otazník (*?*) reprezentuje jeden znak, zatímco hvězdička (***) reprezentuje celý řetězec znaků.

• Pokud chcete vyloučit ve vybrané složce všechny soubory a podsložky, zadejte cestu ke složce a použijte masku *
• Pokud chcete vyloučit všechny .doc soubory, použijte masku **.doc*
• Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční písmeno (řekněme "D"), použijte následující formát:
D????.exe (otazníky nahrazují chybějící a neznámé znaky)
Příklady:
• *C:\Tools** – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce včetně jejich podložek.
• *C:\Tools*.** – se bude chovat stejně jako *C:\Tools**
• *C:\Tools* – v tomto případě nedojde k vyloučení složky *Tools*. Z pohledu skeneru může *Tools* představovat rovněž název souboru.
• *C:\Tools*.dat* – tímto vyloučíte všechny .dat nacházející se ve složce *Tools*.
• *C:\Tools\sg.dat* – vyloučí konkrétní soubor v přesně definované cestě.

Při vytváření výjimek můžete použít systémové proměnné jako *%PROGRAMFILES%*.
• Pro vyloučení složky Program Files pomocí této systémové proměnné použijte cestu *%PROGRAMFILES%** (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty).
• Pokud chcete vyloučit všechny soubory z podsložky *%PROGRAMFILES%*, použijte cestu *%PROGRAMFILES%\vyloučená_složka**

Rozbalte seznam podporovaných systémových proměnných

Při definování výjimky podle cesty můžete použít následující proměnné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Systémové proměnné specifické pro uživatele (jako *%TEMP%* nebo *%USERPROFILE%*) nebo proměnné prostředí (jako *%PATH%*) nejsou podporovány.

Důrazně nedoporučujeme používání zástupných znaků uprostřed cesty (například *C:\Tools*\Data\file.dat*), pokud to nevyžaduje infrastruktura systému. Další informace naleznete v následujícím článku Databáze znalostí.
V případě detekčních výjimek neexistují žádná omezení pro použití zástupných znaků uprostřed cesty.

Pořadí výjimek:
• Pro výjimky nelze nastavovat prioritu pomocí tlačítek nahoru/dolů (jako u pravidel firewallu, kde se pravidla provádějí shora dolů).
• Když skener použije první platné pravidlo, druhé platné pravidlo nebude vyhodnoceno.
• Čím méně pravidel, tím lepší je výkon kontroly.
• Vyhněte se vytváření souběžných pravidel.

Formát výjimky podle cesty

Pro vyloučení skupiny souborů z kontroly můžete použít zástupné znaky. Otazník (*?*) reprezentuje jeden znak, zatímco hvězdička (***) reprezentuje celý řetězec znaků.

• Pokud chcete vyloučit ve vybrané složce všechny soubory a podsložky, zadejte cestu ke složce a použijte masku *
• Pokud chcete vyloučit všechny .doc soubory, použijte masku **.doc*
• Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční písmeno (řekněme "D"), použijte následující formát:
D????.exe (otazníky nahrazují chybějící a neznámé znaky)
Příklady:
• *C:\Tools** – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce včetně jejich podložek.
• *C:\Tools*.** – se bude chovat stejně jako *C:\Tools**
• *C:\Tools* – v tomto případě nedojde k vyloučení složky *Tools*. Z pohledu skeneru může *Tools* představovat rovněž název souboru.
• *C:\Tools*.dat* – tímto vyloučíte všechny .dat nacházející se ve složce *Tools*.
• *C:\Tools\sg.dat* – vyloučí konkrétní soubor v přesně definované cestě.

Při vytváření výjimek můžete použít systémové proměnné jako *%PROGRAMFILES%*.
• Pro vyloučení složky Program Files pomocí této systémové proměnné použijte cestu *%PROGRAMFILES%** (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty).
• Pokud chcete vyloučit všechny soubory z podsložky *%PROGRAMFILES%*, použijte cestu *%PROGRAMFILES%\vyloučená_složka**

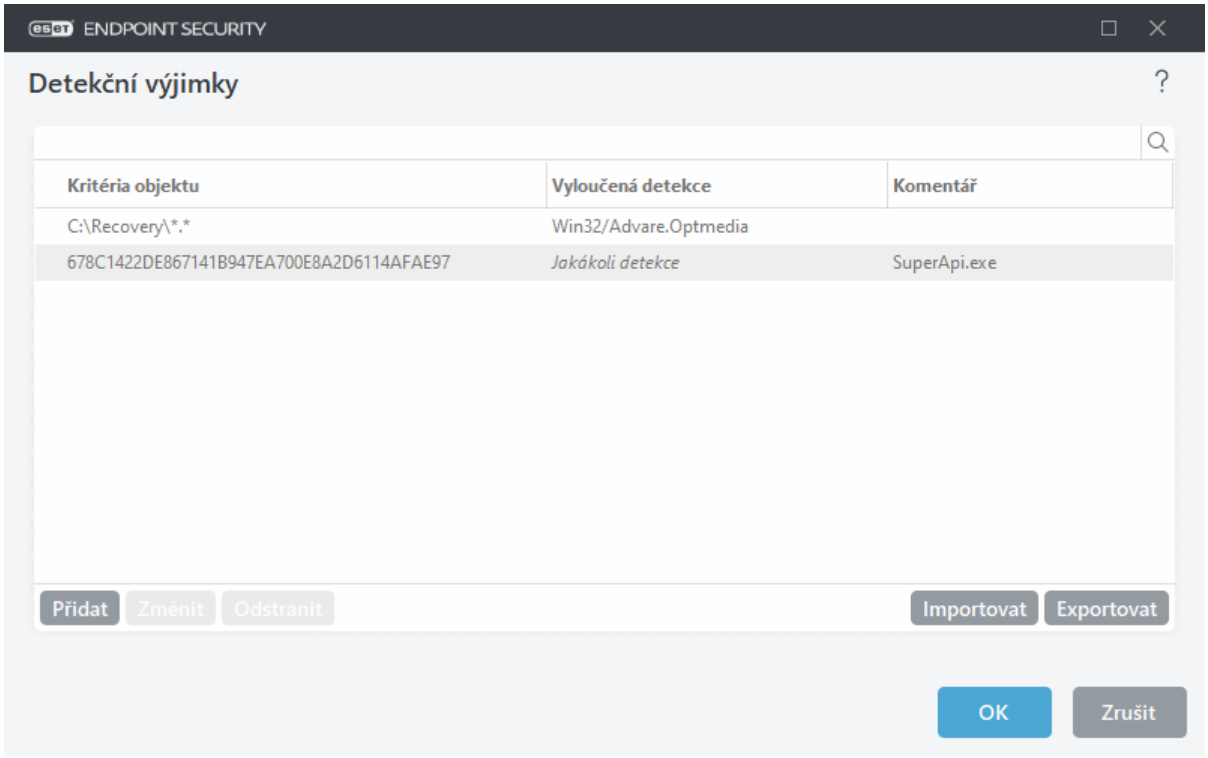
Rozbalte seznam podporovaných systémových proměnných

Při definování výjimky podle cesty můžete použít následující proměnné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Systémové proměnné specifické pro uživatele (jako *%TEMP%* nebo *%USERPROFILE%*) nebo proměnné prostředí (jako *%PATH%*) nejsou podporovány.

Detekční výjimky

Prostřednictvím detekčních výjimek můžete zabránit v léčení objektů tím, že je budete filtrovat na základě názvu detekce, cesty k objektu nebo kontrolního součtu.

Detekční výjimky se nechovají stejně jako Výkonnostní výjimky, které slouží k vyloučení souborů nebo složek z kontroly. Objekt se vyloučí v případě, že je zachycen detekčním jádrem a vyhovuje některému z pravidel uvedených na seznamu detekčních výjimek.
Například podle prvního řádku dle obrázku níže bude z detekčního jádra vyloučen objekt detekovaný jako Win32/Adware.Optmedia, a může se nacházet v umístění *C:\Recovery\file.exe*. Dle druhého řádku bude soubor s uvedeným SHA-1 kontrolním součtem vyloučen bez ohledu na název detekce.



Chcete-li zajistit, aby byly všechny objekty kontrolovány na možný výskyt hrozeb, doporučujeme výjimky vytvářet pouze v nezbytných případech.

Přidání souborů a složek do seznamu výjimek z kontroly provedete v Rozšířených nastaveních > **Detekční jádro** > **Výjimky** > **Detekční výjimky** > **Změnit**.

Pro vyloučení objektu (na základě názvu detekce nebo kontrolního součtu) z léčení klikněte na tlačítko **Přidat**.

Výjimku pro potenciálně nechtěné aplikace a potenciálně zneužitelné aplikace na základě jejich názvu můžete vytvořit rovněž následujícím způsobem:

- V dialogovém okně s upozorněním na detekci klikněte na **Zobrazit rozšířená nastavení** a vyberte možnost **Vyloučit z detekce**.
- V kontextové menu nad konkrétním záznamem v protokolu detekcí použijte Průvodce vytvořením detekční výjimky.
- V hlavním okně programu na záložce **Nástroje** > **Karanténa** klikněte pravým tlačítkem myši na soubor v karanténě a z kontextového menu vyberte možnost **Obnovit a vyloučit z kontroly**.

Kritéria objektu detekční výjimky

- **Cesta** – pomocí této možnosti můžete omezit, v případě potřeby, výjimku jen na konkrétní umístění.
- **Název detekce** – pokud je u vyloučeného souboru uveden i název detekce, znamená to, že je soubor vyloučen pro danou detekci, nikoli celý. Pokud však bude soubor infikován později jiným malwarem, bude detekován.
- **Has** – pomocí této možnosti vyloučíte konkrétní objekt na základě jeho specifického SHA-1 kontrolního součtu bez ohledu na jeho umístění, název nebo příponu.

Ovládací prvky

- **Přidat** – kliknutím přidáte nový záznam na seznam objektů vyloučených z léčení.
- **Změnit** – kliknutím upravíte vybraný záznam.
- **Odstranit** – odstraní vybranou položku (CTRL + klik pro výběr více položek).
- **Import** / **Export** – importování a exportování detekčních výjimek je užitečné například pokud si potřebujete zálohovat stávající seznam výjimek, a chcete se k němu později vrátit. Export nastavení oceníte také v případě nespravovaných prostředí, kdy pro zajištění stejné konfigurace na více počítačích postačí pouze naimportovat daný .txt soubor.

  Zobrazit příklad formátu souboru

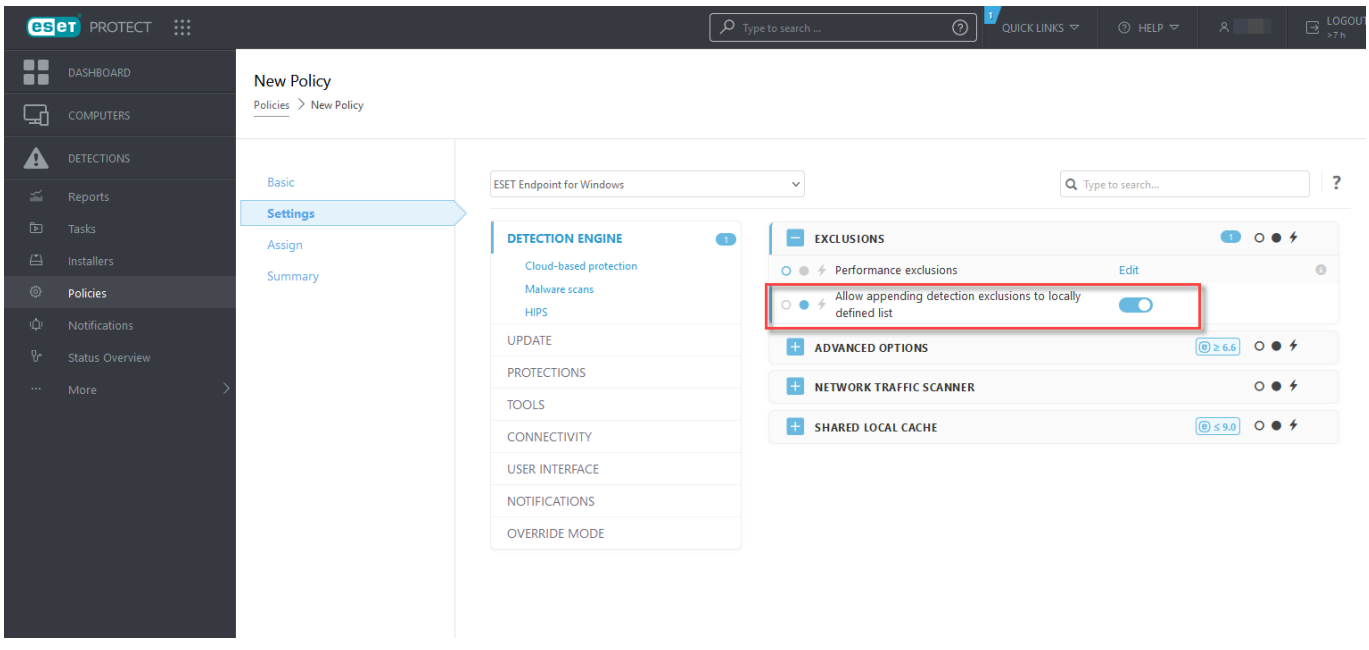
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}

4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF

2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Nastavení detekčních výjimek v ESET PROTECT

Průvodce pro správu nastavení výjimek v ESET PROTECT – vytvořte detekční výjimku a použijte ji pro více zařízení nebo skupin.

Možné riziko přepsání lokálních detekčních výjimek z ESET PROTECT

Pokud se na lokální stanici nacházejí detekční výjimky, pro jejich zachování je nezbytné, aby administrátor ESET_PROTECT v politice aktivoval možnost **Povolit přidání detekčních výjimek k lokálním seznamům**. Poté bude přidání detekčních výjimek definovaných v ESET PROTECTESMC fungovat dle očekávání.

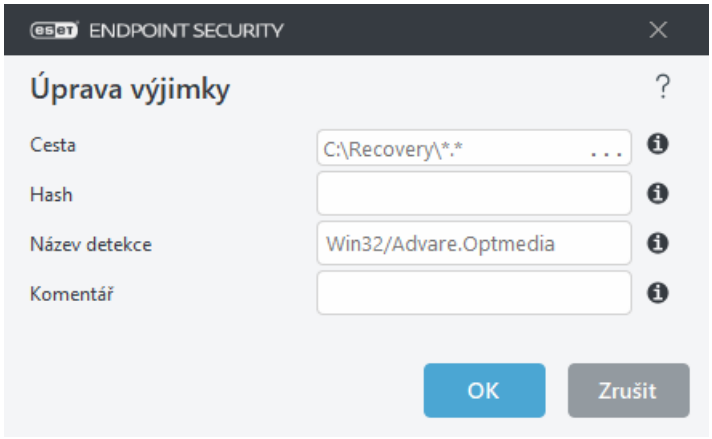


Přidání a úprava detekčních výjimek

Vyloučení detekce

Je nutné uvést platný název ESET detekce. Informace o platném názvu detekce naleznete na záložce Protokoly, kdy z rozbalovacího menu vyberte možnost **Detekce**. Tento typ detekce je vhodné využít v případě, kdy ESET Endpoint Security objekt nesprávně označil za škodlivý (false positive). Protože výjimky pro skutečné infiltrace představují velké riziko, při jejich vytváření zvažte, zda není vhodné vytvořit výjimku pouze na konkrétní soubor nebo umístění, ve kterém k detekci došlo (k tomu využijte tlačítko **…** v poli **Cesta**). Případně výjimku vytvořte pouze dočasně. Výjimky je možné vytvářet také pro potenciálně nechtěné aplikace, potenciálně zneužitelné aplikace a podezřelé aplikace.

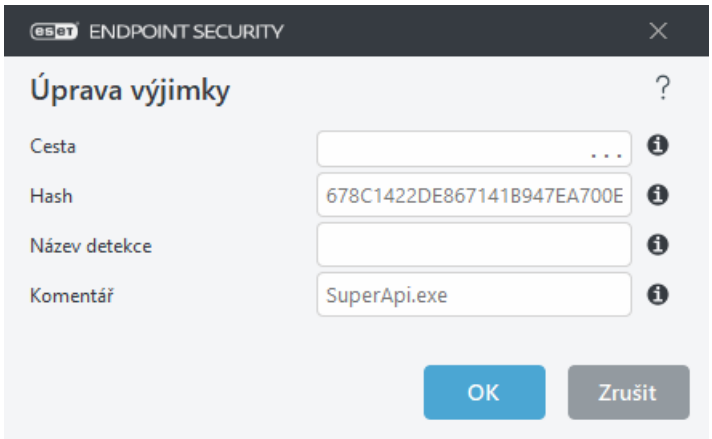
Další informace naleznete v kapitole Formát výjimky podle cesty.



Další informace naleznete v níže uvedeném příkladu na vyloučení detekce.

Vyloučit hash

Pomocí této možnosti vyloučí konkrétní objekt na základě jeho specifického SHA-1 kontrolního součtu bez ohledu na jeho umístění, název nebo příponu.



Pro vyloučení konkrétní detekce na základě názvu zadejte její platný název:
Win32/Adware.Optmedia
Můžete také použít následující formát, pokud vyloučíte detekci z okna výstrahy ESET Endpoint Security:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Ovládací prvky

- **Přidat** – přidá objekt na seznam výjimek.
- **Změnit** – kliknutím upravíte vybraný záznam.
- **Odstranit** – odstraní vybranou položku (CTRL + klik pro výběr více položek).

Průvodce vytvořením detekční výjimky

Detekční výjimku můžete vytvořit také přímo z Protokolu (tato možnost není dostupná nad objekty, které byly označeny jako malware):

1. V hlavním okně programu přejděte na záložku **Nástroje** > **Protokoly**.
2. Z rozbalovacího menu vyberte možnost **Detekce** a následně klikněte pravým tlačítkem na zobrazený záznam.
3. Vyberte možnost **Vytvořit výjimku**.

Pro změnu **Kritéria výjimky** klikněte na tlačítko **Změnit kritéria**.

- **Konkrétní soubory** – pomocí této možnosti vyloučíte konkrétní soubor podle jeho SHA-1 kontrolního součtu.
- **Detekce** – vyloučí soubor podle názvu detekce.
- **Cesta + Detekce** – pomocí této možnosti vyloučíte v konkrétním souboru (například *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*) definovanou detekci.

Na základě typu detekce je vždy předvybrána doporučená možnost.

Volitelně můžete přidat **Komentář**, pokračujte kliknutím na tlačítko **Vytvořit výjimku**.

Rozšířená nastavení detekčního jádra

Zapnout rozšířenou kontrolu prostřednictvím AMSI – pokud zapnete tuto možnost v Rozšířených nastaveních > Detekční jádro > Další možnosti, bude nástroj Antimalware Scan Interface (AMSI) kontrolovat skripty PowerShellu, skripty spouštěné programem Windows Script Host a data kontrolovaná pomocí AMSI SDK.

Kontrola síťové komunikace

Kontrola síťové komunikace poskytuje ochranu před malwarem pro aplikační protokoly, která integruje několik pokročilých technik kontroly škodlivého kódu. Kontrola síťové komunikace automaticky kontroluje protokoly

HTTP(S), POP3(S) a IMAP(S) bez ohledu na internetový prohlížeč nebo e-mailového klienta. Kontrolu síťové komunikace můžete zapnout nebo vypnout v Rozšířeném nastavení > **Detekční jádro** > **Kontrola síťové komunikace**.

Zapnout kontrolu síťové komunikace – pokud tuto možnost vypnete, protokoly HTTP(S), POP3(S) a IMAP(S) se nebudou kontrolovat. Všimněte si, že následující funkce ESET Endpoint Security vyžadují zapnutou Kontrolu síťové komunikace:

- Ochrana přístupu na web
- Prostřednictvím Filtrování obsahu webu
- Zabezpečený prohlížeč
- SSL/TLS
- Anti-Phishingová ochrana
- Ochrany poštovních klientů,

Cloudová ochrana

ESET LiveGrid® (nová generace systému včasného varování ESET ThreatSense.Net) využívá data od uživatelů bezpečnostních produktů ESET z celého světa a zasílá je do virových laboratoří společnosti ESET. Díky podezřelým vzorkům a souvisejícím metadatům dokážeme prostřednictvím ESET LiveGrid® okamžitě reagovat na nejnovější hrozby.

K dispozici jsou následující možnosti:

Možnost 1: Zapnutí reputačního systému ESET LiveGrid®

Reputační systém ESET LiveGrid® porovnává soubory v cloudu oproti neškodnému nebo škodlivému chování souborů.

Díky tomuto systému máte možnost ověřit přímo z rozhraní produktu ESET, případně kontextového menu, spolehlivost souborů a spuštěných procesů a získat o těchto objektech další informace ze systému ESET LiveGrid®.

Možnost 2: Zapnutí systému zpětné vazby ESET LiveGrid®

Na rozdíl od reputačního systému ESET LiveGrid®, shromažďuje systém zpětné vazby ESET LiveGrid® z vašeho počítače pouze informace, které se týkají nové infiltrace. To může zahrnovat vzorek nebo kopii souboru, ve kterém se infiltrace objevila, název složky, kde se soubor nacházel, název souboru, informaci o datu a času detekce, způsob, jakým se infiltrace dostala do počítače, a informaci o používaném operačním systému.

Ve výchozí konfiguraci ESET Endpoint Security odesílá na podrobnou analýzu do virové laboratoře ESET pouze podezřelé soubory. Pokud se infiltrace nachází v souborech s určitými příponami, jako například *.doc* nebo *.xls*, nikdy se neodesílá jejich obsah. Mezi výjimky můžete přidat další přípony souborů, jejichž obsah nechcete odesílat.

Možnost 3: Můžete se rozhodnout ESET LiveGrid® nezapínat

Tím nepřijdete o žádnou funkci v programu. Pokud ale ESET LiveGrid® zapnete, může ESET Endpoint Security v některých případech reagovat na nové hrozby dříve, než nedojde k aktualizaci detekčního jádra.

Více informací o technologii ESET LiveGrid® naleznete ve slovníku pojmů.
Názorné ukázky, jak zapnout nebo vypnout ESET LiveGrid® v produktu ESET Endpoint Security máme k dispozici v Databázi znalostí v angličtině několika dalších jazycích.

Konfigurace cloudové ochrany v Rozšířeném nastavení produktu

Chcete-li získat přístup k nastavení ESET LiveGrid®, otevřete Rozšířená nastavení > **Detekční jádro** > **Cloudová ochrana**.

Zapnout reputační systém ESET LiveGrid® (doporučeno) – reputační systém ESET LiveGrid® zvyšuje účinnost anti-malwarových řešení ESET ověřováním souborů vůči cloudové databázi povolených a zakázaných souborů.

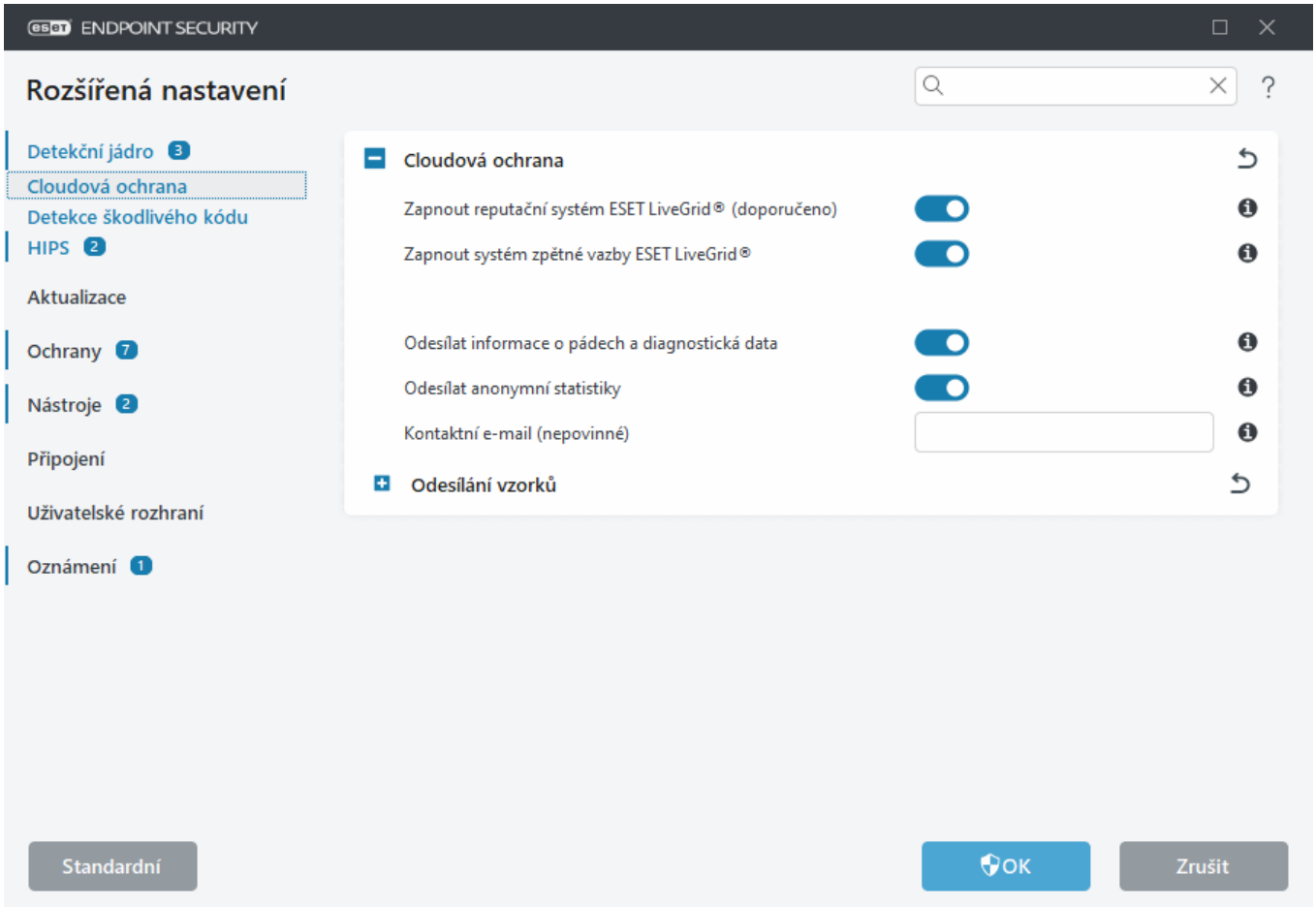
Zapnout systém zpětné vazby ESET LiveGrid® – po aktivování se budou do laboratoří ESET k analýze odesílat relevantní data (popsáno níže v sekci **Odesílání vzorků**) společně se statistikami a hlášeními o pádech.

Zapnout ESET LiveGuard (ESET LiveGuard je doplňková funkce prodávaná společností ESET a není ve výchozím nastavení k dispozici) – ESET LiveGuard je placená služba poskytovaná společností ESET. Jedná o další ochranou vrstvu navrženou pro snížení dopadu zcela nových hrozeb. Funguje tak, že podezřelé soubory jsou automaticky odesílány k analýze do cloudového systému společnosti ESET. V cloudu se v průběhu jejich analyzování využívají pokročilé detekční techniky. Uživatel následně obdrží souhrnný přehled o chování zaslaného vzorku.

Odesílat informace o pádech a diagnostická data – po aktivování ESET LiveGrid® se budou odesílat diagnostická data, jako jsou informace o pádech a výpisy obsahu paměti jednotlivých modulů. Doporučujeme ponechat tuto funkci zapnutou, abyste pomohli firmě ESET diagnostikovat problémy, vylepšovat produkty a zajistit lepší ochranu uživatelů.

Odesílat anonymní statistiky – tímto umožníte společnosti ESET shromažďovat informace o nově detekovaných hrozbách, jako je název hrozby, datum a čas detekce, metoda detekce a přidružená metadata, verze produktu a konfigurace včetně informací o vašem systému.

Kontaktní e-mail (nepovinný údaj) – zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.



Odesílání vzorků

Ruční odesílání vzorků – umožňuje z kontextového menu, Karantény nebo z části Nástroje > Další nástroje odesílat soubor k analýze do společnosti ESET.

Automatické odesílání detekovaných vzorků

Vyberte, jaké druhy vzorků budete odesílat do společnosti ESET k analýze a za účelem vylepšení detekce. K dispozici jsou následující možnosti:

- **Všechny detekované vzorky** – všechny objekty detekované Detekčním jádrem (včetně potenciálně nechtěných aplikací, pokud je jejich detekce v nastavení skeneru povolena).
- **Všechny vzorky kromě dokumentů** – všechny detekované objekty kromě **Dokumentů** (viz níže).
- **Neodesílat** – Detekované objekty nebudou společnosti ESET odeslány.

Automatické odesílání podezřelých souborů

Tyto vzorky budou rovněž poslány společnosti ESET i v případě, že nebudou detekovány detekčním jádrem. Například vzorky, které se vyhnuly detekci těsně, nebo je některý z modulů ochrany ESET Endpoint Security považuje za podezřelé, nebo mají podezřelé chování.

- **Spustitelné soubory** – zahrnuje následující typy souborů: .exe, .dll, .sys.
- **Archivy** – zahrnuje následující typy souborů: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skripty** – zahrnuje následující typy souborů: .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Ostatní** – zahrnuje následující typy souborů: .jar, .reg, .msi, .sfw, .lnk.
- **Pravděpodobný spam** – vybráním této možnosti umožníte zasílání částí nebo celých zpráv, včetně příloh,

označených jako spam k bližší analýze do společnosti ESET. Tímto krokem přispějete k vylepšení globální detekce nevyžádaných e-mailů, a získáte tím, nejen vy, v budoucnu lepší detekci spamu.

- **Dokumenty** – zahrnují dokumenty Microsoft Office nebo PDF s aktivním obsahem i bez něj.

  Zobrazit seznam všech dotčených typů dokumentů

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Výjimky

Pomocí filtru výjimek můžete vyloučit složky a konkrétní typy souborů z odeslání k analýze (například soubory obsahující citlivé informace jako dokumenty nebo tabulky). Soubory uvedené na seznamu nebudou nikdy odeslány do laboratoří ESET k analýze, i pokud by se v nich nacházel škodlivý kód. Standardně jsou vyloučeny nejrozšířenější typy souborů (.doc, atp.). Do seznamu výjimek můžete přidat vlastní typy souborů.

Pro vyloučení souborů stažených z download.domain.com, otevřete Rozšířená nastavení > **Cloudová ochrana** > **Odesílání vzorků** > **Výjimky** a přidejte vyloučení *download.domain.com*.

Maximální velikost vzorku (MB) – určuje maximální velikost automaticky odesílaných vzorků (1-64 MB).

ESET LiveGuard

ESET LiveGuard na klientské stanici aktivujete prostřednictvím ESET PROTECT Web Console. Více informací naleznete v kapitole Konfigurace ESET LiveGuard v ESET Endpoint Security.

Pokud jste měli zapnutý ESET LiveGrid® a nyní jste jej vypnuli, může se stát, že v počítači jsou již připraveny datové balíčky k odeslání. Tyto balíčky se ještě odešlou při nejbližší příležitosti. Po vypnutí systému se již nové balíčky vytvářet nebudou.

Filtr výjimek pro cloudovou ochranu

Pomocí seznamu výjimek můžete zabránit v odesílání konkrétních typů souborů nebo obsahu složek k analýze. Soubory uvedené na seznamu nebudou nikdy odeslány do laboratoří ESET k analýze, i pokud by se v nich nacházel škodlivý kód. Standardně se neodesílají nejrozšířenější typy souborů (.doc, atp.).

Tuto funkci můžete využít pro vyloučení souborů, které by mohly obsahovat důvěryhodné informace – například dokumenty nebo tabulky.

Pro vyloučení souborů stažených z adresy download.domain.com přejděte v Rozšířeném nastavení do sekce **Detekční jádro** > **Cloudová ochrana** > **Odesílání vzorků**. Na řádku **Výjimky** klikněte na Změnit a v zobrazeném dialogovém okně definujte výjimku následovně: *download.domain.com*.

Detekce škodlivého kódu

Sekce **Detekce škodlivého kódu** je přístupná z Rozšířeného nastavení > **Detekční jádro** > **Detekce škodlivého kódu** a umožňuje konfigurovat parametry pro profily kontroly.

Volitelná kontrola

Profil kontroly – určuje název profilu, jehož nastavení se použijí při volitelné kontrole počítače. Nový profil můžete vytvořit po kliknutí na tlačítko **Změnit** na řádku **Seznam profilů**. Další podrobnosti naleznete v kapitole Profily kontroly.

Po výběru profilu kontroly můžete nakonfigurovat následující možnosti:

Cíle kontroly – pokud chcete zkontrolovat konkrétní cíl nebo skupinu cílů, klikněte na **Změnit** vedle položky **Cíle kontroly** a vyberte možnost ze stromové struktury složek. Další podrobnosti naleznete v kapitole Cíle kontroly.

Volitelná ochrana s využitím strojového učení – pro každý profil kontroly můžete nakonfigurovat úrovně hlášení a ochrany. Ve výchozím nastavení mají profily kontroly stejné nastavení, jaké je nastaveno v části Rezidentní ochrana souborového systému. Pro konfiguraci vlastních hlášení a úrovní ochrany přepínačem deaktivujte možnost **Použít nastavení rezidentní ochrany**. Podrobné vysvětlení úrovní hlášení a ochrany naleznete v kapitole Ochrany.

ThreatSense – možnosti v Rozšířeném nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole ThreatSense.

Profily kontroly

K dispozici jsou čtyři předdefinované profily kontroly ESET Endpoint Security:

- **Smart kontrola počítače**: toto je výchozí profil pokročilé kontroly. Profil Smart kontrola počítače využívá technologii Smart optimalizace, pro vyloučení souborů, které byly při předchozí kontrole označeny jako čisté, a nedošlo u nich od té doby ke změně. Tím se zkracuje doba kontroly při současném minimálním dopadu na zabezpečení systému.
- **Kontrola z kontextového menu**: Volitelnou kontrolu libovolného souboru můžete spustit z kontextového menu. Profil kontroly z kontextového menu umožňuje nastavit konfiguraci kontroly při jejím využití.
- **Hloubková kontrola počítače**: Profil hloubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.
- **Kontrola počítače**: Toto je výchozí profil používaný při standardní kontrole počítače.

Oblíbená nastavení kontroly počítače si můžete uložit do profilů pro jejich opakované použití v budoucnu. Doporučujeme vytvořit několik profilů s různými cíli a metodami kontroly, případně s dalšími parametry.

Pro vytvoření nového profilu otevřete Rozšířená nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** > **Seznam profilů** > **Změnit**. Kliknutím na **Změnit** na řádku **Seznam profilů** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. Chcete-li si vytvořit profil kontroly, který bude vyhovovat vašim potřebám, podívejte se do kapitoly ThreatSense, kde najdete popis jednotlivých parametrů pro nastavení kontroly.

> Chcete si vytvořit vlastní profil **kontroly počítače** a částečně vám vyhovuje nastavení předdefinovaného profilu, ale nechcete zároveň kontrolovat runtime packery nebo potenciálně nebezpečné aplikace a zároveň **Vždy vyřešit infekci**? V **Seznamu profilů** klikněte na tlačítko **Přidat** a profil pojmenujte. Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktualizační profil** nastavte si parametry kontroly podle potřeby, a změny uložte kliknutím na tlačítko OK.

Cíle kontroly

Prostřednictvím rozbalovacího menu **Cíle kontroly** můžete vybrat ke kontrole předdefinované cíle.

- **Podle nastavení profilu** – vybere cíle nastavené ve vybraném profilu kontroly.
- **Výměnné disky** – vybere diskety, USB flash disky, CD/DVD.
- **Lokální disky** – vybere lokální pevné disky v počítači.
- **Síťové disky** – vybere namapované síťové disky.
- **Vlastní výběr** – zruší výběr cílů.

Další cíle kontroly si můžete vybrat ve stromové struktuře.

- **Operační paměť** – kontrola všech procesů a dat aktuálně nahraných v operační paměti.
- **Boot sektory/UEFI** – kontrola přítomnosti škodlivého kódu v boot sektorech disků a UEFI. Pro více informací o UEFI skeneru přejděte do slovníku pojmů.
- **WMI databáze** – kontrola celé Windows Management Instrumentation (WMI) databáze, všech jmenných prostorů, tříd instancí a vlastností. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor.
- **Registr systému** – kontrola celého registru systému, všech klíčů a podklíčů. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor. Při léčení detekce zůstane v registru odkaz, aby se zabránilo ztrátě důležitých dat.

Pro rychlý přesun k požadovanému cíli kontroly (souboru nebo složce), zadejte jeho cestu do textového pole zobrazeném pod stromovou strukturou. Mějte na paměti, že se v cestě rozlišuje velikost písmen. Použitím zaškrtávacího pole ve stromové struktuře přidáte daný cíl do seznamu cílů, které se mají kontrolovat.

Kontrola při nečinnosti

Kontrolu při nečinnosti můžete nastavit v Rozšířeném nastavení v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Kontrola při nečinnosti**.

Kontrola při nečinnosti

Aktivujte tuto funkci pomocí přepínače vedle položky **Zapnout kontrolu při nečinnosti**. Tichá kontrola všech lokálních disků v počítači se spouští v případě, že je počítač ve stavu nečinnosti.

Standardně se kontrola při nečinnosti nespouští, pokud je počítač (notebook) napájen z baterie. Toto nastavení můžete zrušit aktivací přepínače vedle položky **Spustit také při napájení počítače z baterie** v Rozšířeném nastavení.

V Rozšířeném nastavení přepínačem aktivujte možnost **Zapisovat do protokolu**, pokud chcete průběh kontroly zapisovat do sekceProtokoly (v hlavním okně programu klikněte na **Nástroje** > **Protokoly** a z rozbalovacího menu**Detekce** vyberte možnost **Kontrola počítače**).

Detekce stavu nečinnosti

Více informací o možnostech definování akce, při které se spustí kontrola, naleznete v kapitole Detekce stavu nečinnosti.

ThreatSense – možnosti v Rozšířeném nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole ThreatSense.

Detekce stavu nečinnosti

Nastavení Detekce stavu nečinnosti můžete konfigurovat v části Rozšířené nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Kontrola při nečinnosti** > **Detekce stavu nečinnosti**. Tato nastavení určují spouštění Kontroly při nečinnosti:

- **Vypnutí obrazovky nebo spuštění spořiče obrazovky**,
- **Uzamčení počítače**,
- **Odhlášení uživatele**,

Pomocí přepínačů určete stav, při kterém chcete provádět kontrolu počítače.

Kontrola po startu

Standardně se kontrola souborů zaváděných při startu počítače do operační paměti provádí během startu počítače a po aktualizaci detekčního jádra. Tato kontrola závisí na nastavení úloh v Plánovači.

Možnosti nastavení kontroly souborů zaváděných při startu počítače jsou součástí naplánované úlohy **Kontrola souborů spouštěných po startu**. Chcete-li upravit toto nastavení, přejděte na **Nástroje** > **Plánovač** > klikněte na **Kontrola souborů spouštěných po startu** a následně na tlačítko **Změnit**. V posledním kroku se zobrazí okno Kontrola souborů spouštěných po startu počítače. Více informací o tvorbě a správě úloh Plánovače naleznete v kapitole Vytvoření nové úlohy.

ThreatSense – možnosti v Rozšířeném nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole ThreatSense.

Automatická kontrola souborů spouštěných při startu počítače

Při vytvoření naplánované úlohy zajišťující kontroly souborů spouštěných při startu operačního systému můžete vybírat z níže uvedených parametrů.

Pomocí rozbalovacího menu **Cíle kontroly** můžete upravit množství souborů, které se má kontrolovat. Seznam souborů, získaný na základě sofistikovaného algoritmu, je seřazen vzestupně podle následujících kritérií:

- **Všechny registrované soubory** (nejvíce kontrolovaných souborů)
- **Málo používané soubory**
- **Běžně používané soubory**
- **Často používané soubory**
- **Pouze nejčastěji používané soubory** (nejméně kontrolovaných souborů)

Mezi tyto možnosti patří také tyto dvě:

- **Soubory zaváděné před přihlášením uživatele** – zahrnuje soubory z míst, ke kterým může být přistupováno

bez toho, aby byl uživatel přihlášen (typicky všechny položky po spuštění jako jsou služby, browser helper objects, winlogon oznámení, záznamy plánovače Windows, známé dll atd.).
- **Soubory zaváděné po přihlášení uživatele** – zahrnuje soubory z míst, ke kterým může být přistupováno až po přihlášení uživatele (typicky soubory, které jsou spouštěny pro daného uživatele, nejčastěji umístěné v *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*.

Seznamy souborů určených ke kontrole jsou určeny výše uvedenými skupinami. Pokud zvolíte nižší hloubku kontroly pro soubory spouštěných při startu, nebudou kontrolovány po otevření nebo spuštění.

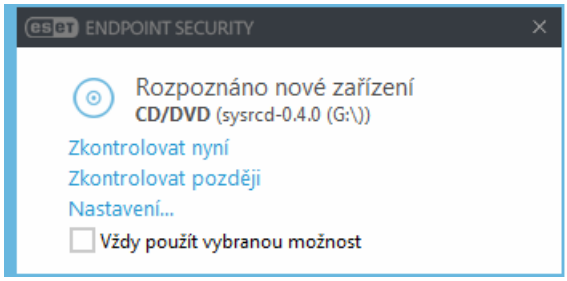
Priorita kontroly – definujte úroveň priority, při které se spustí kontrola počítače:

- **Při nečinnosti** – úloha se spustí pouze při nečinnosti systému,
- **Nižší** – zatížení systému je nižší,
- **Nejnižší** – zatížení systému je nejnižší,
- **Normální** – zatížení systému je běžné.

Výměnná média

ESET Endpoint Security dokáže automaticky kontrolovat výměnná média (CD/DVD/USB/...) po jejich vložení/připojení do počítače. Tuto funkci můžete využít, pokud jako správce počítače chcete zabránit uživatelům v používání škodlivého obsahu na výměnných médií.

Pokud je vloženo výměnné médium a v Rozšířeném nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média** je nastavena možnost **Zobrazit možnosti kontroly**, objeví se následující dialogové okno:



Možnosti tohoto dialogu:

- **Zkontrolovat nyní** – spustí se ruční kontrola výměnného média.
- **Nekontrolovat** – po vybrání této možnosti se výměnné médium nezkontroluje.
- **Nastavení** – otevře Rozšířená nastavení.
- **Vždy použít vybranou možnost** – pokud vyberete toto pole, při příštím připojení výměnného média se provede stejná akce.

Kromě toho Správa zařízení ESET Endpoint Security disponuje pokročilými funkcemi, které vám umožňují definovat pravidla pro zacházení s externími zařízeními připojovanými k vašemu počítači. Více informací naleznete v kapitole Správa zařízení.

K přístupu do nastavení kontroly výměnných médií otevřete Rozšířená nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média**.

Akce po vložení vyměnitelného média – Vyberte výchozí akci, která bude provedena po vložení vyměnitelného

média do počítače (CD/DVD/USB). Po vložení výměnného média do počítače vyberte požadovanou akci:

- **Nekontrolovat** – neprovede se žádná akce a upozornění **Nalezeno nové nařízení** se nezobrazí.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí kontrola jeho obsahu.
- **Vynucená kontrola zařízení** – po vložení média se automaticky spustí kontrola jeho obsahu, kterou nelze přerušit.
- **Zobrazit možnosti kontroly** – otevře možnost **Nastavení výměnných médií**.

Ochrana dokumentů

Modul ochrany dokumentů zajišťuje kontrolu dokumentů Microsoft Office před jejich otevřením a také kontroluje automaticky stahované soubory pomocí Internet Explorer, jako například prvky Microsoft Microsoft ActiveX. Tento modul přidává další bezpečnostní vrstvu do rezidentní ochrany a může být deaktivován pro zvýšení výkonu systému, na kterém neotevíráte velké množství dokumentů Microsoft Office.

Pro zapnutí této možnosti přejděte do Rozšířeného nastavení > **Detekční jádro** > **Detekce škodlivého kódu** > **Ochrana dokumentů** a klikněte na přepínač vedle **Zapnout ochranu dokumentů**.

ThreatSense – možnosti v Rozšířeném nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole ThreatSense.

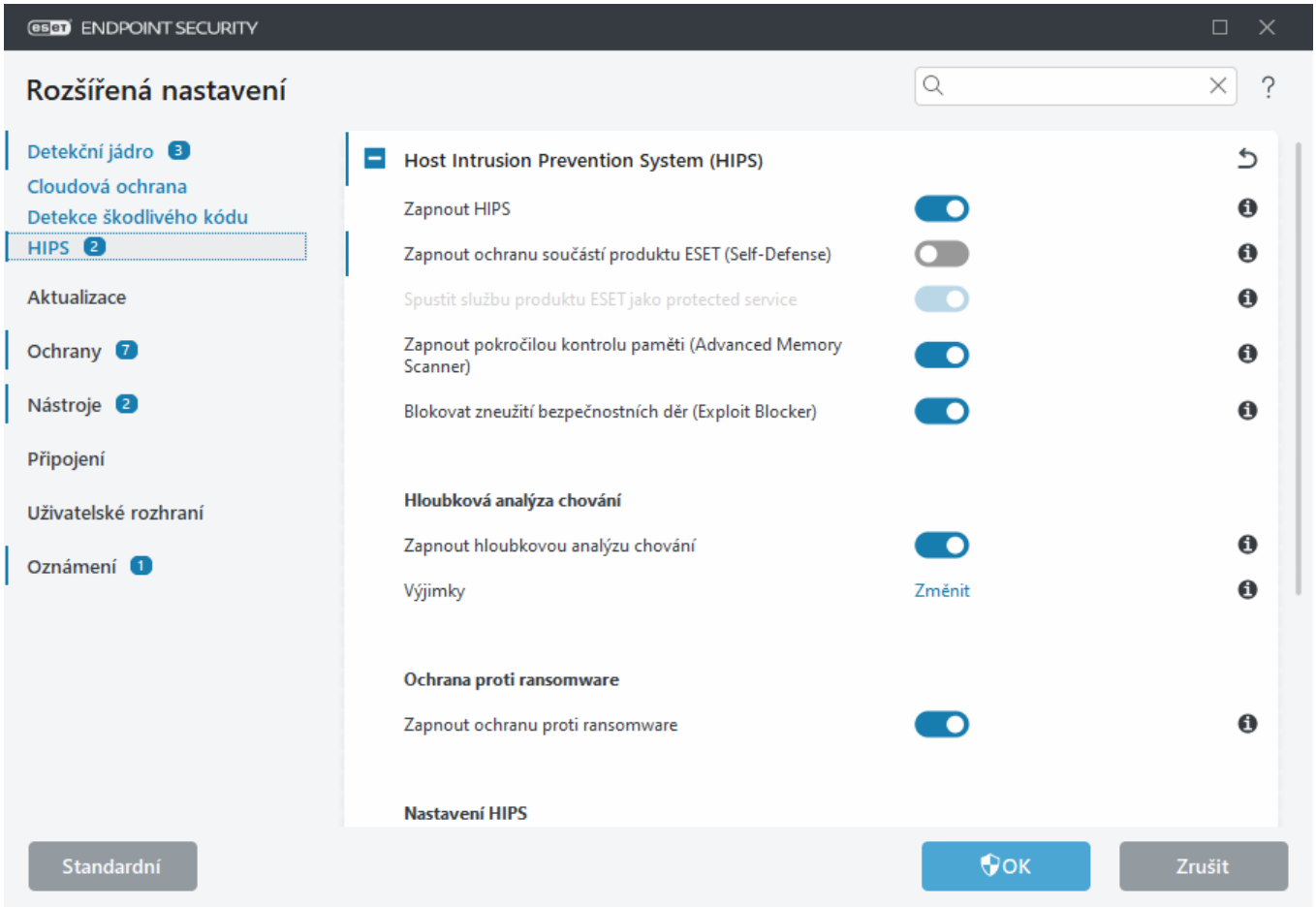
Tento modul pracuje pouze s aplikacemi, které podporují rozhraní Microsoft Antivirus API (například Microsoft Office 2000 a novější nebo Microsoft Internet Explorer 5.0 a novější).

HIPS – Host-based Intrusion Prevention System

Pokud nejste zkušený uživatel, nedoporučujeme měnit nastavení systému HIPS. Chybnou úpravou nastavení HIPS se může systém stát nestabilní.

Host-based Intrusion Prevention System (HIPS) chrání operační systém před škodlivými kódy a eliminuje aktivity ohrožující bezpečnost počítače. HIPS používá pokročilou analýzu chování kódu, která spolu s detekčními schopnostmi síťového filtru zajišťuje efektivní kontrolu běžících procesů, souborů a záznamů v registru Windows. HIPS je nezávislý na rezidentní ochraně a firewallu a monitoruje pouze běžící procesy v operačním systému.

Sysém HIPS můžete nastavit v Rozšířených nastaveních > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)**. Stav modulu HIPS je zobrazen v hlavním okně programu ESET Endpoint Security > **Nastavení** > **Počítač**.



Host Intrusion Prevention System (HIPS)

Zapnout HIPS – HIPS je v ESET Endpoint Security standardně zapnutý. Jeho vypnutím zakážete běh dalších součástí HIPS jako je například Exploit Blocker.

Zapnout ochranu součástí produktu ESET (Self-Defense) – ESET Endpoint Security obsahuje vestavěnou technologii **Self-Defense**, která brání škodlivé aplikaci v narušení nebo zablokování antivirové ochrany. Self-Defense chrání soubory a klíče v registru, které jsou kritické pro správnou funkci produktu ESET a neumožňuje potenciálnímu škodlivému software přístup k těmto záznamům a procesům a jejich úpravu. Rovněž chrání ESET Management Agenta, pokud je nainstalován.

Spustit službu produktu ESET jako protected service – pomocí této možnosti zapnete ochranu služby ESET (ekrn.exe). Pokud je možnost zapnutá, služba je spuštěná jako chráněný proces ve Windows a slouží tak pro boj se škodlivým kódem. Tato možnost je dostupná ve Windows 8.1 a Windows 10.

Zapnout pokročilou kontrolu paměti (Advanced Memory Scanner) – tato funkce v kombinaci s blokováním zneužití bezpečnostních děr (Exploit Blocker) poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.

Blokovat zneužití bezpečnostních děr (Exploit Blocker) – tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, PDF čtečky a komponenty Microsoft Office). Tato funkce je standardně zapnuta. Více informací o této vrstvě ochrany naleznete ve slovníku pojmů.

Hloubková analýza chování

Hloubková analýza chování je další vrstvou ochrany funkce HIPS. Toto rozšíření analyzuje chování běžících programů a varuje vás, jestliže jejich chování bude pro váš počítač škodlivé.

HIPS výjimky Hloubkové analýzy chování umožňují vyloučit procesy z kontroly. Pro zajištění všech kontrol na možné hrozby doporučujeme vytvářet vyloučení pouze v případě, že je absolutně nezbytné.

Ochrana proti ransomware

Zapnout ochranu proti ransomware – tato součást představuje další vrstvu funkce HIPS. Pro správnou funkci ochrany proti ransomware je třeba mít zapnutý Reputační systém ESET LiveGrid®. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.

Zapnout Intel® Threat Detection Technology – technologie pomáhá odhalovat útoky ransomwaru využitím unikátní telemetrie z procesoru Intel. Zvyšuje účinnost detekce, snižuje počet falešných poplachů a rozšiřuje možnosti zachycení pokročilých technik na obcházení detekce v paměti zařízení. Viz podporované procesory.

Zapnout auditování – po aktivování auditování nebudou detekované hrozby ochranou proti ransomware blokovány, pouze dojde k jejich zaznamenání do protokolu s úrovní varování a do konzole pro správu budou reportovány s příznakem "REŽIM AUDITU". Jako administrátor se následně rozhodněte, zda pro detekci vytvoříte výjimku. Pokud detekci ponecháte aktivní, po ukončení režimu auditu dojde k zablokování a odstranění detekovaného objektu. Zapnutí/vypnutí režimu auditu se zaznamená do protokolu ESET Endpoint Security. Nicméně tato možnost je dostupná pouze v konfiguračním editoru ESET PROTECT při vytváření politiky.

Nastavení HIPS

HIPS může běžet v jednom z následujících **režimů**:

Režim filtrování	Popis
Automatický režim	Operace budou povoleny s výjimkou blokovaných na základě předdefinovaných pravidel, které váš systém chrání.
Smart režim	Uživatel bude upozorněn pouze na velmi podezřelé události.
Interaktivní režim	Uživatel bude na povolení operace dotázán.
Administrátorský režim	Blokuje každé spojení, pro které neexistuje povolující pravidlo.
Učící režim	Operace jsou povoleny a po každé operaci je vytvořeno pravidlo. Pravidla vytvořená v tomto režimu jsou viditelná v editoru **Pravidel HIPS**, ale jejich priorita je nižší než priorita pravidel vytvořených ručně nebo pravidel vytvářených v automatickém režimu. Vyberete-li v rozbalovací nabídce **Režim filtrování** možnost **Učící režim**, zpřístupní se nastavení **Učící režim bude ukončen**. Vyberte časové období (max. 14 dní), pro které bude učící režim aktivní. Po uplynutí zadaného období budete vyzváni k úpravě pravidel vytvořených pomocí HIPS v učícím režimu. Můžete také zvolit jiný režim filtrování nebo odložit rozhodnutí a pokračovat v používání režimu učení.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte režim filtrování, který se automaticky nastaví po ukončení běhu učícího režimu. Pokud vyberete možnost **Dotázat se uživatele**, pro změnu režimu filtrování modulu HIPS bude vyžadováno oprávnění administrátora.

Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům firewallu. Kliknutím na **Změnit** vedle položky **Pravidla** otevřete editor **Pravidla HIPS**. Zde

můžete pravidla prohlížet, vytvářet nová, upravovat nebo odstranit stávající. Více detailů o vytváření pravidel a operacích HIPS naleznete v kapitole Úprava pravidla HIPS.

HIPS výjimky

Prostřednictvím výjimek můžete vyloučit procesy z HIPS Hloubkové analýzy chování.

Chcete-li upravit výjimky pro HIPS, otevřete Rozšířená nastavení > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)** > **Výjimky** > **Změnit**.

> Nezaměňujte tuto funkci s možností pro vyloučení přípon souborů z kontroly, tvorbu detekčních výjimek, výkonnostních výjimek, vyloučených procesů.

Pro vyloučení objektu z kontroly klikněte na tlačítko **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury. Existující výjimky můžete upravovat, případně odstranit.

Rozšířená nastavení HIPS

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

Automaticky povolené ovladače – seznam ovladačů, které budou vždy načteny, bez ohledu na nastavený režim filtrování, pokud nejsou blokovány uživatelským pravidlem.

Zapisovat všechny zablokované operace do protokolu – všechny zablokované operace se zapíší do protokolu HIPS. Tuto možnost aktivujte výhradně na výzvu specialisty technické podpory ESET. Mějte na paměti, že se následně začne generovat velké množství dat a může dojít ke zpomalení počítače.

Upozornit na změny v seznamu aplikací automatický spouštěných při startu – při změně počtu aplikací spouštěných po startu operačního systému se zobrazí oznámení.

Ovladače, jejichž načtení je vždy povoleno

Vybrané ovladače budou vždy načteny bez ohledu na nastavený režim filtrování modulu HIPS, pokud nejsou blokovány uživatelským pravidlem.

Přidat – přidá nový ovladač.

Změnit – upraví parametry vybraného ovladače.

Odstranit – odebere ovladač ze seznamu.

Reset – obnoví seznam na výchozí hodnoty.

> Po kliknutí na tlačítko **Obnovit** vymažete všechny ovladače, které jste přidali ručně. V seznamu zůstanou pouze systémové ovladače.

> Po instalaci je seznam ovladačů prázdný. ESET Endpoint Security je časem automaticky doplní.

Ovladače, které se vždy mohou načíst, jsou specifické pro každé zařízení a nelze je upravovat pomocí politik ESET PROTECT. Po instalaci je seznam ovladačů prázdný. ESET Endpoint Security je časem automaticky doplní.

Interaktivní režim HIPS

Přímo z okna HIPS oznámení můžete vytvořit pravidlo na základě akce, které modul HIPS detekoval, a definovat podmínky, za kterých bude tato operace povolena nebo blokována.

Pravidla vytvořená z oznámení jsou ekvivalentní ručně vytvořeným. Pravidlo vytvořené z oznámení může být však méně specifické, než pravidlo vytvořené prostřednictvím editoru pravidel. To znamená, že po vytvoření pravidla prostřednictvím editoru může stejná operace vyvolat zobrazení oznámení. Pro více informací si nastudujte prioritu HIPS pravidel.

Pokud je jako výchozí akce pro pravidlo nastavena možnost **Vždy se dotázat**, dialogové okno se zobrazí při každé aktivaci pravidla. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**. Pokud v danou chvíli akci nevyberete, nová akce se vybere na základě pravidel.

Aktivovaná možnost **Dočasně si zapamatovat akci pro tento proces** způsobí, že se vybraná akce (**Povolit nebo Zakázat**) zapamatuje pro tento proces, a použije se pokaždé, kdyby se pro operaci tohoto procesu měl zobrazit další dotazovací dialog. Tato nastavení jsou jen dočasná, platí pouze do nejbližší změny pravidel, režimu filtrování, aktualizaci modulu HIPS nebo restartu systému.

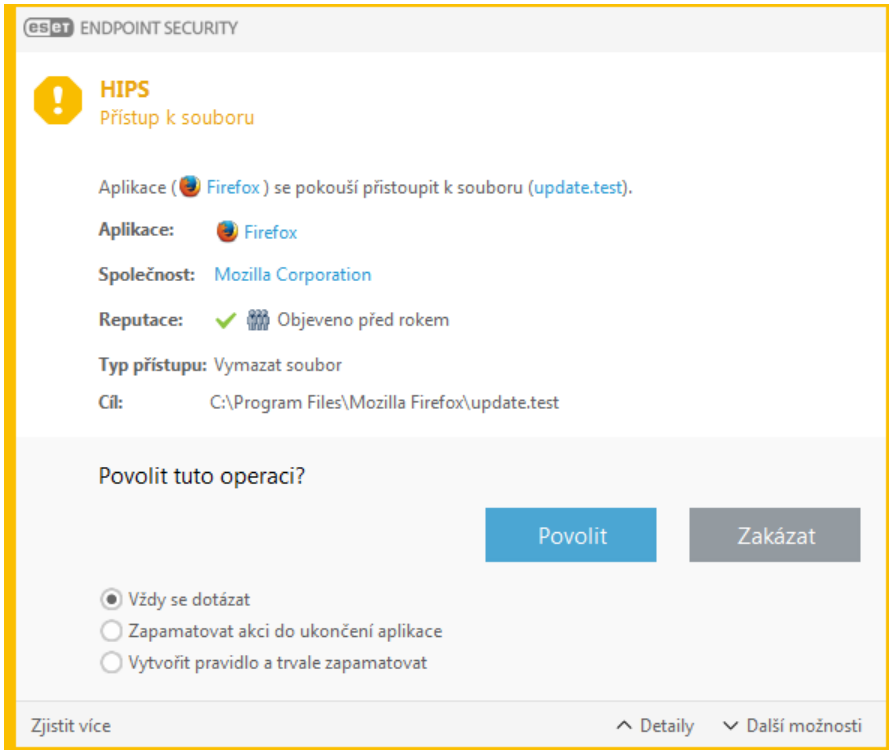
Vybráním možnosti **Vytvořit pravidlo a trvale zapamatovat** vytvoříte nové HIPS pravidlo, kterém můžete následně modifikovat prostřednictvím Editoru HIPS pravidel (ke změně pravidel je vyžadováno oprávnění administrátora).

Kliknutím na **Detaily** v dolní části okna zjistíte, jaká aplikace operaci vyvolala, jakou má soubor reputaci, případně na jaký typ akce (povolit, blokovat) jste byli dotázání.

Nastavení detailních parametrů si zpřístupníte kliknutím na **Rozšířená nastavení**. Níže uvedené možnosti jsou dostupné v případě, kdy vyberte možnost **Vytvořit pravidlo a trvale zapamatovat**.

- **Vytvořit pravidlo platné pouze pro tuto aplikaci** – pokud tuto možnost zrušíte, pravidlo bude platné pro všechny zdrojové aplikace.
- **Pouze pro operaci** – vyberte operaci se souborem/aplikace/registrem. Pro více informací se podívejte na popis všech HIPS operací.
- **Pouze pro cíl** – vyberte, zda bude pravidlo platné pro soubor/aplikaci/registr.

Pro ukončení zobrazování oznámení přepněte režim filtrování na **Automatický režim**. Nastavení provedete v Rozšířeném nastavení v sekci **Detekční jádro** > **HIPS** > **Obecné**.



Detekován potenciální ransomware

Toto dialogové okno se zobrazí, pokud je detekována aplikace, jejíchž chování je velmi podobné ransomware. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**.

Prostřednictvím tohoto dialogového okna můžete **odeslat vzorek do virové laboratoře k bližší analýze**, případně danou aplikaci **vyloučit z detekce**. Po kliknutí na možnost **Detaily** si zobrazíte konkrétní parametry detekce.

Pro fungování ochrany proti ransomware je vyžadována aktivní technologie ESET LiveGrid®.

Správa HIPS pravidel

V tomto dialogovém okně naleznete uživatelsky a automaticky vytvořená pravidla modulu HIPS. Více informací o tvorbě HIPS pravidel naleznete v kapitole Úprava pravidel. Podívejte se rovněž do kapitoly Obecné principy HIPS.

Sloupce

Pravidlo – uživatelský nebo automaticky zadaný název pravidla.

Zapnuto – odškrtněte tuto možnost, pokud chcete ponechat pravidlo v seznamu pravidel, ale nepoužívat ho.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Zdroje – pravidlo se uplatní, pouze pokud událost vyvolají dané aplikace.

Cíle – pravidlo se použije, pouze pokud se operace týká daného cíle (souboru, aplikace nebo záznamu v registru).

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do protokolu HIPS.

Oznámit – pokud je spuštěna událost, zobrazí se v pravém dolním rohu obrazovky oznámení.

Ovládací prvky

Přidat – kliknutím vytvoříte nové pravidlo.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odstraníte vybraný záznam.

Priorita pravidel HIPS

Neexistují žádné možnosti nastavení proirity pravidel HIPS pomocí tlačítek nahoru/dolů (jako u pravidel firewallu, kde se pravidla provádějí shora dolů).

- Všechna pravidla mají stejnou prioritu
- Specifičtější pravidla mají vyšší prioritu (například pravidlo pro konkrétní aplikaci je nadřazeno pravidlu platnému pro všechny aplikace)
- Interně HIPS obsahuje několik předdefinovaných pravidel s nejvyšší prioritou, která nemůžete ovlivnit (například nemůžete přepsat Self-Defense pravidla)
- Vámi vytvořená pravidla, která mohou způsobit zamrznutí systému, se nebudou aplikovat (budou mít nejnižší prioritu)

Úprava pravidla HIPS

Nejprve si prosím pročtěte kapitolu Správa HIPS pravidel.

Název pravidla – uživatelský nebo automaticky zadaný název pravidla.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Operace ovlivní – vyberte typ operace, pro kterou má být pravidlo platné. Konkrétní pravidlo je možné použít pouze pro jeden typ operace nad vybraným cílem.

Zapnuto – deaktivujte tuto možnost pomocí přepínače, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do protokolu HIPS.

Upozornit uživatele – pokud je spuštěna události, zobrazí se v pravém dolním rohu obrazovky oznámení.

Pravidlo se skládá z částí, které definují podmínky, za kterých se pravidlo uplatní.

Zdrojové aplikace – pravidlo se uplatní, pouze pokud událost vyvolají **definované aplikace**. Pro vybrání **konkrétní aplikace** klikněte v rozbalovacím menu na **Přidat** a vyberte jednotlivé soubory nebo klikněte na možnost **Všechny aplikace** pro výběr všech.

Cílové soubory – pravidlo se uplatní pouze v případě, kdy operace náleží cíli. Pro vybrání **konkrétních souborů** klikněte v rozbalovacím menu na možnost **Přidat** a vyberte jednotlivé soubory nebo složky nebo klikněte na **Všechny soubory** pro výběr všech.

Aplikace – pravidlo se uplatní, pouze pokud se operace provádí nad definovanými aplikacemi. Pro vybrání **konkrétní aplikace** klikněte v rozbalovacím menu na **Přidat** a vyberte jednotlivé soubory nebo složky nebo klikněte na možnost **Všechny aplikace** pro výběr všech.

Záznamy registru – pravidlo se uplatní, pouze pokud se operace provádí nad definovanými záznamy v registru. Pro vybrání konkrétních záznamů klikněte na tlačítko **Přidat** a vyberte jednotlivé klíče nebo hodnoty. Pro monitorování celého registru vyberte z rozbalovacího menu možnost **Všechny záznamy**.

Některé operace zvláštních pravidel předefinovaných systémem HIPS nemohou být zablokovány a standardně jsou povoleny. HIPS nemonitoruje všechny systémové operace. HIPS monitoruje operace, které mohou být považovány za nebezpečné.

Při zadání cesty C:\example se pravidlo aplikuje na všechny akce související se složkou. Zadáním C:\example*.* aplikujete pravidlo na všechny soubory uvnitř složky.

Operace aplikace

- **Ladění jiné aplikace** – připojení debuggeru k procesu. Při debuggingu můžete sledovat a měnit chování aplikace a přistupovat k jejím datům.
- **Zachytávat události jiné aplikace** – zdrojová aplikace se pokouší zachytit události cílové aplikace (například pokud se keylogger snaží zachytit aktivitu webového prohlížeče).
- **Ukončit/přerušit jinou aplikaci** –pozastavení, obnovení nebo ukončení procesu (může být vyvoláno přímo ze Správce úloh nebo ze záložky Procesy).
- **Spustit novou aplikaci** – spuštění nové aplikace nebo procesu.
- **Změnit stav jiné aplikace** – zdrojová aplikace se pokouší zapisovat do paměti cílové aplikace, případně se snaží spustit kód pod jejím jménem. Tato funkce je užitečná pro ochranu důležité aplikace, pokud ji nastavíte jako cílovou aplikaci v pravidle, které blokuje tyto operace.

Operace se záznamy registru

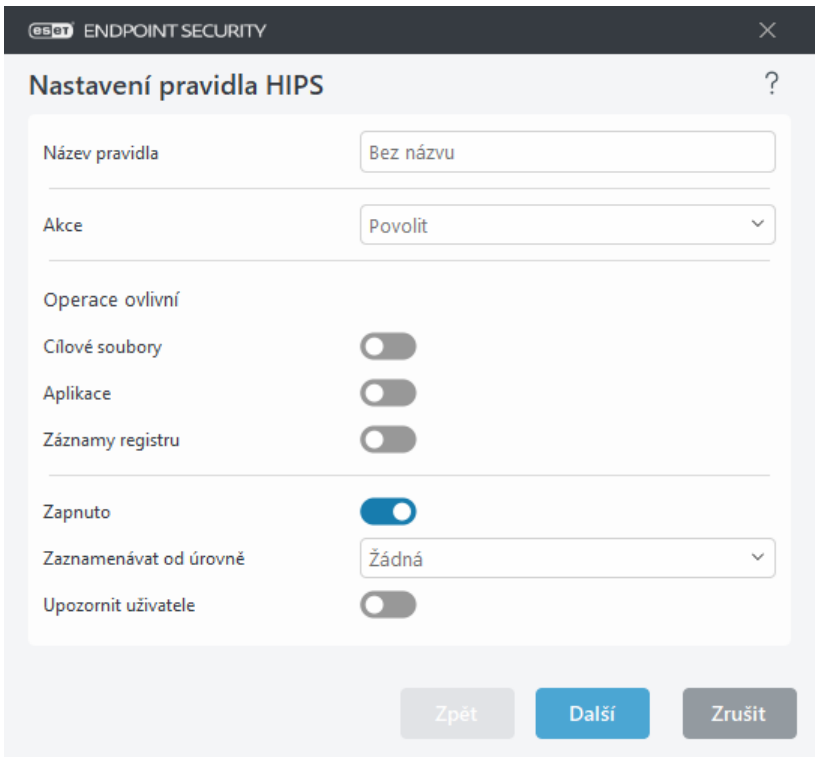
- **Úprava nastavení spuštění** – všechny změny v nastavení, definující, které aplikace budou spouštěny při startu operačního systému Windows. Zobrazíte je například vyhledáním klíče Run v Editoru registru Windows
- **Vymazání z registru** – vymazání klíče nebo hodnoty.
- **Přejmenování klíče registru** – přejmenování konkrétního klíče.
- **Úprava registru** – vytvoření nové hodnoty nebo změna existujících hodnot. Přesouvání dat v rámci datové struktury. Nastavení uživatelských nebo skupinových práv pro dané klíče registru.

Použití zástupných znaků v pravidlech
Hvězdičku můžete v pravidlech použít pouze jako náhradu konkrétního klíče, například "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start". Ostatní možnosti použití zástupných znaků nejsou podporovány.
Vytvoření pravidla na klíč v HKEY_CURRENT_USER
Tento klíč je pouze odkaz směřující na podklíč HKEY_USERS konkrétního uživatele reprezentovaný SID (secure identifier). Pro vytvoření pravidla pouze na aktuálního uživatele použijte místo HKEY_CURRENT_USER cestu směřující na HKEY_USERS\%SID%. Jako SID můžete použít také hvězdičku, a dojde k aplikování pravidla na všechny uživatele.

⚠ Pokud vytvoříte příliš obecné pravidlo, program vás na to upozorní.

Na následujícím příkladu si ukážeme, jak omezit nežádoucí chování aplikací:

1. Zadejte název pravidla a z rozbalovacího menu **Akce** vyberte **Blokovat** (nebo **Dotázat se**, pokud se chcete při výskytu akce rozhodnout později).
2. Zapněte možnost **Upozornit uživatele** pro zobrazení upozornění při každém aplikování pravidla.
3. V části **Operace ovlivní** vyberte alespoň jednu operaci, pro kterou má pravidlo platit.
4. Pokračujte kliknutím na tlačítko **Další**.
5. V dialogovém okně **Zdrojové aplikace** vyberte možnost **Konkrétní aplikace**. Tím zajistíte, že vámi vytvářené pravidlo bude platné pouze pro konkrétní aplikace.
6. Klikněte na tlačítko **Přidat** a **…**. Výběr cesty k aplikaci potvrďte kliknutím na tlačítko **OK**. V případě potřeby přidejte více aplikací.
   Příklad: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Jako operaci vyberte **Zápis do souboru**.
8. V dalším kroku vyberte z rozbalovacího menu **Všechny soubory**. Tím zablokujete jakýkoli pokus definovaných aplikací o zápis do libovolného souboru.
9. Vytvoření nového pravidla potvrdíte kliknutím na tlačítko **OK**.



Přidat cestu k aplikaci/registru pro HIPS

Kliknutím na **…** vyberte cestu k aplikaci. Pokud vyberete složku, všechny aplikace v této složce budou zahrnuty do daného pravidla.

Kliknutím na **Otevřít Editor registru** spustíte Editor registru Windows (regedit). Během přidávání zadejte správnou cestu do pole **Hodnota**.

Příklad cesty k souboru nebo v registru:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Aktualizace

Možnosti nastavení aktualizace jsou k dispozici v Rozšířeném nastavení > **Aktualizace**. Tato sekce vám poskytne informace o aktualizačních serverech a datech pro tyto servery.

Pro správné fungování aktualizace je nezbytné zadat veškeré aktualizační informace správně. Pokud používáte firewall, ujistěte se, že program ESET má povolenou komunikaci s internetem (například komunikaci HTTPS).

Aktualizace

Aktuálně používaný aktualizační profil se zobrazuje v rozbalovacím menu **Vyberte výchozí profil aktualizace**.

Pro vytvoření nového profilu přejděte do kapitoly Profily aktualizace.

Automatické přepínání profilu – pomocí této možnosti můžete Známým sítím definovaným ve Firewallu přiřadit konkrétní aktualizační profil. Pomocí této funkce se může profil automaticky přepínat na základě sítě, do které je zařízení připojeno. Pro více informací se podívejte do uživatelské příručky.

Konfigurace oznámení o aktualizacích – klikněte na Změnit a následně si vyberte oznámení, která chcete, aby aplikace zobrazovala. Rozhodnout se můžete, zda chcete oznámení Zobrazit na ploše a/nebo Odeslat e-mailem.

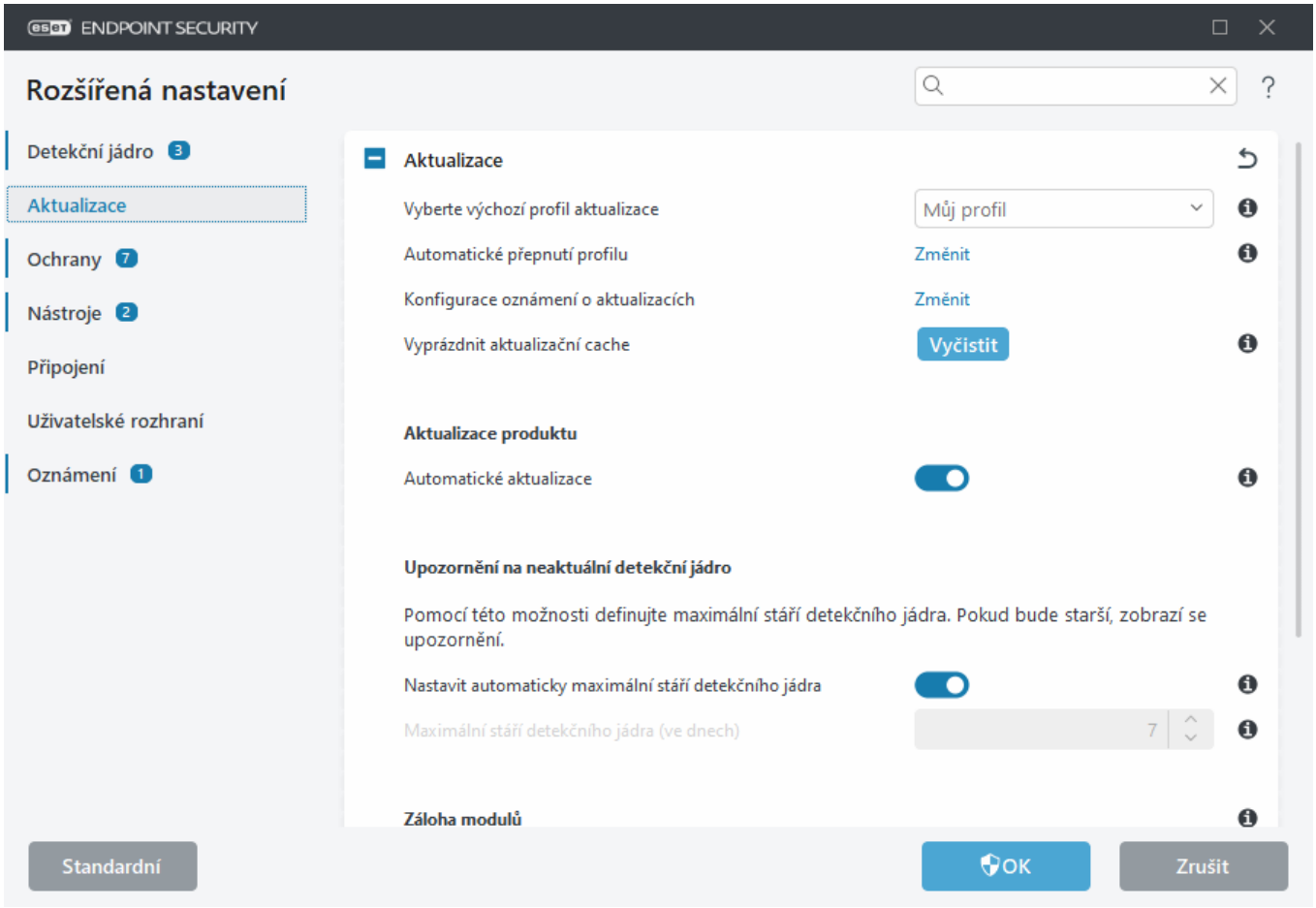
Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit** na řádku **Vyprázdnit aktualizační cache**.

Upozornění na neaktuální detekční jádro

Nastavit automaticky maximální stáří detekčního jádra – pomocí této možnosti nastavíte maximální přístupné stáří detekčního jádra. Bude-li starší, zobrazí se informace, že detekční jádro není aktuální. Výchozí hodnota pro **Maximální stáří detekčního jádra** je 7 dní.

Záloha modulů

Pokud máte podezření, že nová verze detekčního jádra je nestabilní nebo poškozená, můžete se vrátit ke starší verzi modulů a na stanovený časový interval zakázat její aktualizaci.



Profily

Aktualizační profily můžete použít pro různá nastavení aktualizací. Vytvoření aktualizačních profilů pro aktualizaci má význam především pro mobilní uživatele, kteří si mohou vytvořit alternativní profil pro internetové připojení, které se často mění.

V rozbalovacím menu **Aktualizační profil** se vždy zobrazuje aktuálně vybraný profil. Standardně je vybrán profil s názvem **Můj profil**.

Pro vytvoření nového klikněte na **Změnit** vedle položky **Seznam profilů**, následně klikněte na tlačítko **Přidat** a zadejte **Název profilu**.

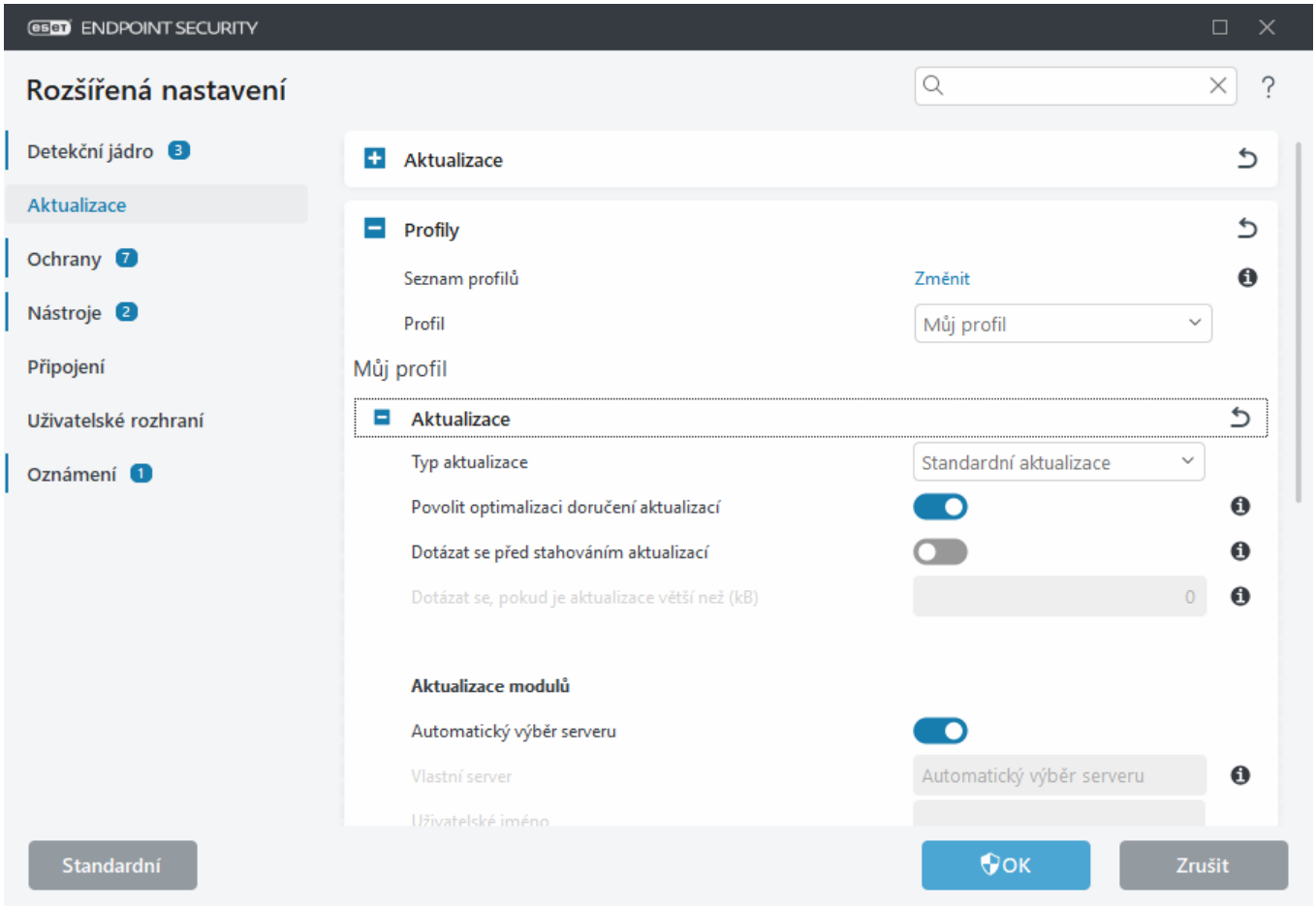
Aktualizace

Jako **Typ aktualizace** je ve výchozím nastavení vybrána možnost **Standardní aktualizace**. Tím je zajištěno automatické stahování aktualizací ze serverů společnosti ESET. **Předběžné aktualizace** jsou aktualizace, které prošly důkladným interním testováním a budou brzy dostupné široké veřejnosti. Při vybrání této možnosti získáte v předstihu přístup k novějším opravám a metodám detekce škodlivého kódu. Protože předběžné aktualizace nereprezentují finální kvalitu, neměli byste je instalovat na produkční stroje a pracovní stanice, u kterých je vyžadována stabilita a dostupnost. Opožděné aktualizace – vybráním této možnosti se aktualizace budou stahovat z aktualizačního serveru, na který jsou umísťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

Povolit optimalizaci doručení aktualizací – po aktivování této možnosti se mohou aktualizační soubory stahovat z CDN (content delivery network). Po vypnutí tohoto nastavení však může dojít ke zpomalení nebo přerušení stahování, pokud budou dedikované servery společnosti ESET přetížené. Toto nastavení zároveň deaktivujte,

pokud máte na svém firewallu povolen výhradně přístup na aktualizační servery ESET na základě jejich IP adres. V takovém případě se klienti nebudou schopni připojit k CDN službě.

Dotázat se před stahováním aktualizací – zapne zobrazování oznámení, ve kterém lze zvolit, zda aktualizaci chcete přijmout nebo odmítnout. V případě, že aktualizační soubor bude větší, než mezní hranice definovaná v poli Dotázat se, pokud je velikost aktualizačního souboru větší než (kB), program zobrazí oznámení. Pokud je velikost aktualizačního souboru nastavena na 0 kB, program zobrazí potvrzovací dialog vždy.



Aktualizace modulů

Standardně je aktivní možnost **Automatický výběr serveru**. Pokud chcete program aktualizovat ze serverů společnosti ESET, ponechte tuto možnost beze změny. V opačném případě ji deaktivujte, a do pole Vlastní server zadejte ručně adresu k vašemu aktualizačnímu serveru.

Zapnout častější aktualizace detekčních signatur – aktivováním této možnosti se budou detekční signatury aktualizovat v kratších intervalech. Deaktivace tohoto nastavení může mít negativní dopad na rychlost detekce.

Povolit aktualizaci modulů z výměnného média – po aktivování této možnosti můžete koncový produkt aktualizovat z výměnného média, pokud do kořene nakopírujete obsah vašeho aktualizačního mirroru. Vybráním možnosti Automaticky dojde k aktualizaci na pozadí po připojení výměnného média. Pokud chcete nejprve zobrazit upozornění na možnost aktualizace, vyberte možnost Vždy se dotázat.

Pokud používáte lokální HTTP server, aktualizační server by měl být zadán následovně:
http://nazev_pocitace_nebo_jeho_IP_adresa:2221

Pokud používáte lokální HTTP server s SSL šifrováním, aktualizační server by měl být zadán následovně:
https://nazev_pocitace_nebo_jeho_IP_adresa:2221

Pokud používáte lokální sdílenou složku, aktualizační server by měl být zadán následovně:

*nazev_pocitace_nebo_jeho_IP_adresa**sdilena_slozka*

Číslo portu HTTP serveru použité v příkladu se může v závislosti na vaší konfiguraci lišit.

Aktualizace produktu

Pro více informací přejděte do kapitoly Aktualizace produktu.

Možnosti připojení

Pro více informací přejděte do kapitoly Možnosti připojení.

Mirror

Pro více informací přejděte do kapitoly Aktualizační mirror.

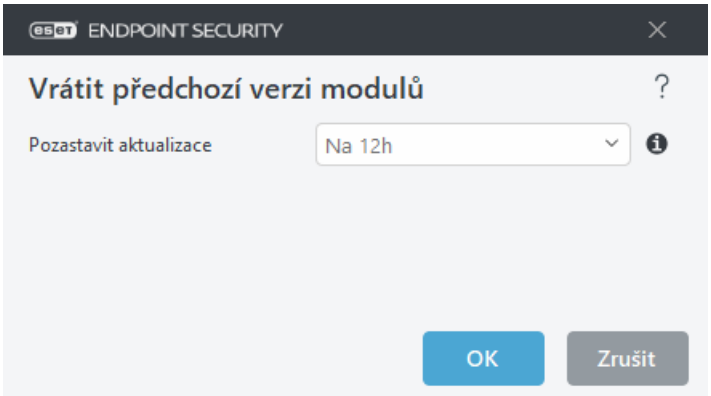
Obnovení předchozí verze modulů

Pokud máte podezření, že nová verze detekčního jádra je nestabilní nebo poškozená, můžete se vrátit ke starší verzi a na stanovený časový interval zakázat jejich aktualizaci. Případně můžete povolit dříve zakázané aktualizace, pokud jste je odložili na neomezeně dlouhou dobu.

ESET Endpoint Security zálohuje detekční jádro a programové moduly pro případ, že by bylo potřeba se vrátit ke starší verzi. Aby se obrazy, tzv. snapshoty modulů, vytvářely, ponechte možnost **Vytvářet zálohu modulů** aktivní. Po jejím **zapnutí** se první záloha (snapshot) vytvoří v průběhu příští aktualizace. Další záloha se následně vytvoří po uplynutí 48 hodin. **Počet vytvářených záloh** určuje počet obrazů detekčního jádra uložených na lokálním disku počítače.

Při dosažení maximálního počtu vytvářených záloh (například tří), dojde každých 48 hodin k nahrazení nejstarší zálohy novou. ESET Endpoint Security se při obnovení předchozí verze detekčního jádra a programových modulů vrátí vždy k nejstarší verzi.

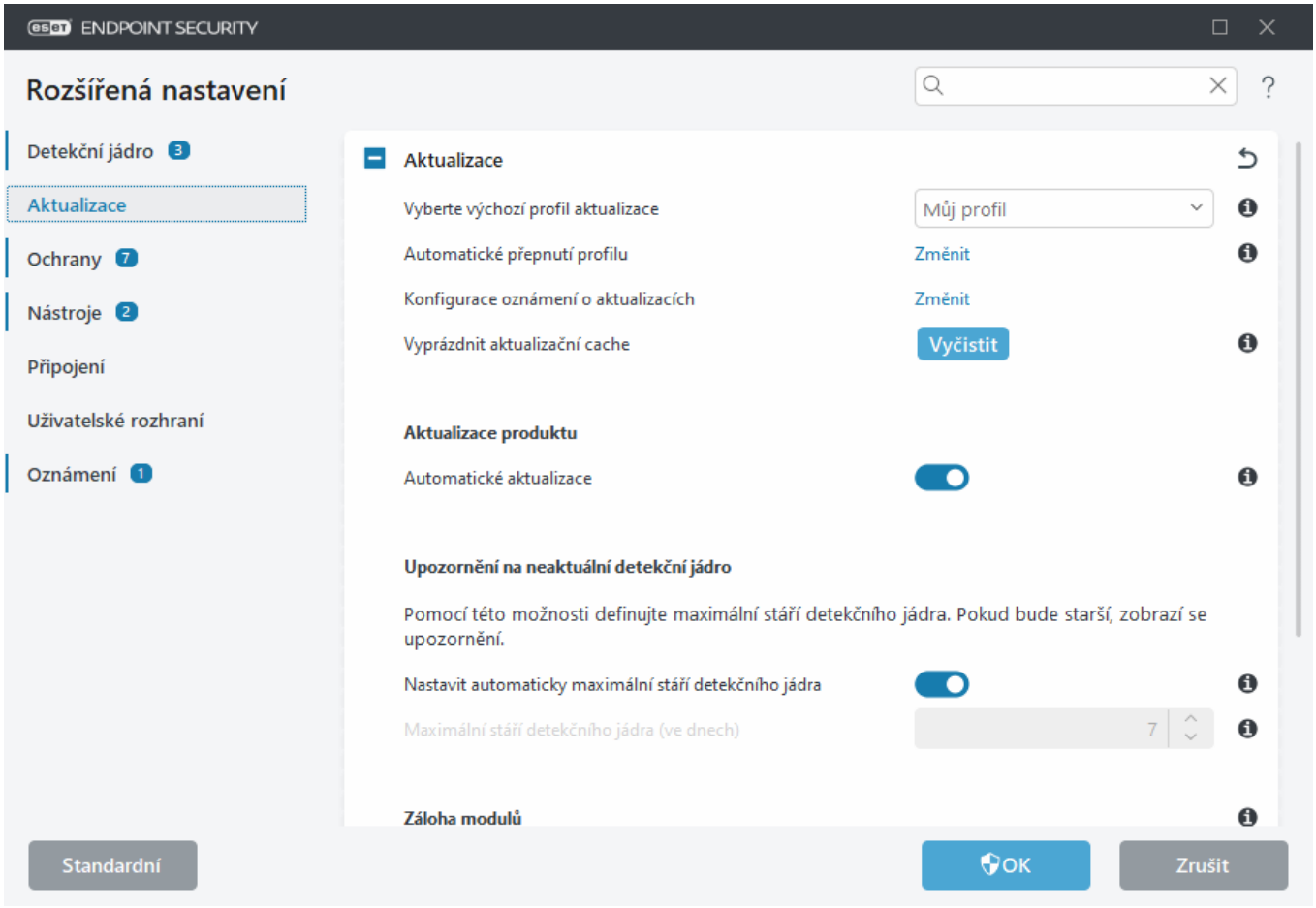
Otevřete Rozšířená nastavení > **Aktualizace** > **Obecné** > **Záloha modulů** > **Vrátit** a vyberte časový interval z rozbalovacího menu **Doba**.



Možnost **Do odvolání** vyberte v případě, kdy chcete aktualizaci modulů obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Po obnovení předchozí verze modulů se tlačítko **Vrátit** změní, a bude sloužit pro akci **Povolit aktualizace**.

Aktualizace se přeruší na dobu definovanou v dialogovém okně **Pozastavit aktualizace na**. Ze zálohy se obnoví nejstarší verze detekčního jádra a programových modulů uložená v souborovém systému počítače.



Nejnovější verze detekčního jádra má číslo 22700. Na pevném disku počítače jsou uloženy obrazy detekčního jádra 22698 a 22696. Všimněte si, že verze 22697 není k dispozici. Počítač byl totiž delší dobu vypnutý, proto byla stažena novější verze modulů. Pokud jste jako **Počet vytvářených záloh** nastavili číslo 2, po **navrácení změn** se obnoví detekční jádro (i programové moduly) s číslem 22696. Tento proces může chvíli trvat. Pro ověření, zda došlo k obnovení starší verze přejděte v hlavním okně programu na záložku Aktualizace.

Aktualizace produktu

V sekci **Aktualizace produktu** naleznete možnosti související s aktualizací produktu na novou verzi. Můžete zde nastavit akci, která se má stát, pokud je k dispozici nová verze produktu.

Aktualizace produktu přinášejí nové funkce, nebo upravují již existující z předchozích verzích. Aktualizace může probíhat automaticky bez interakce uživatele, nebo po jejím odsouhlasení. Mějte na paměti, že po dokončení aktualizace produktu na novou verzi může být vyžadován restart počítače.

Automatické aktualizace – pozastavením automatických aktualizací v konkrétním aktualizačním profilu dočasně zakážete automatické aktualizace produktu při připojení k internetu pomocí jiných sítí nebo připojení účtovaných podle objemu dat. Pro zajištění neustálého přístupu k nejnovějším funkcím a nejvyšší možné ochrany, je nutné ponechat toto nastavení zapnuté. Další informace týkající se automatických aktualizací naleznete v samostatném FAQ.

Ve výchozím nastavení se aktualizace produktu stahují ze serverů společnosti ESET. Ve velkých sítích nebo offline

prostředí můžete k jejich distribuci využít lokální server.

Vlastní server

1. Cestu k lokálním kopiím aktualizací produktu definujte v poli **Vlastní server**.
Definovat můžete HTTP(S) server, SMB síťové umístění, lokální disk nebo výměnné médium. V případě síťových jednotek doporučujeme použít UNC cestu místo písmena namapované jednotky.
2. Pole **Uživatelské jméno** a **Heslo** ponechte prázdná, pokud není autentifikace vyžadována.
V opačném případě zadejte odpovídající údaje pro ověření přístupu k vašemu vlastnímuHTTP serveru.
3. Uložte změny a otestujte aktualizaci produktu vyvoláním standardní aktualizace produktu ESET Endpoint Security.

Vhodnost použití jednotlivých možností pro aktualizaci produktu závisí na stanici, na které bude nastavení použito. Zde je potřeba si uvědomit odlišnost nastavení při nasazení na serveru oproti pracovní stanici, kde může být například automatický restart v nevhodnou dobu nežádoucí.

Možnosti připojení

Chcete-li získat přístup k možnostem nastavení proxy serveru pro konkrétní profil aktualizace, otevřete Rozšířená nastavení > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení**.

Proxy server

V rozbalovacím menu **Režim proxy** jsou dostupné následující možnosti:

- Nepoužívat proxy server,
- Připojení prostřednictvím proxy serveru,
- Použít globální nastavení proxy serveru.

Vybráním možnosti **Použít globální nastavení proxy serveru** se použijí veškerá nastavení proxy serveru zadaná v Rozšířených nastaveních > **Připojení** > **Proxy server**.

Pomocí možnosti **Nepoužívat proxy server** zajistíte, aby se při aktualizaci ESET Endpoint Security nepoužíval proxy server.

Možnost **Připojení prostřednictvím proxy serveru** vyberte v případě, že:

- Pro aktualizaci ESET Endpoint Security se používá jiný proxy server než ten, který je definován v sekci **Nástroje** > **Proxy server**. Při takové konfiguraci definujte nový proxy server zadáním jeho adresy do pole **Proxy server**, komunikačního portu (standardně 3128), **uživatelského jména** a **hesla** pro přístup k proxy serveru, je-li to potřeba.
- Nastavení proxy serveru není nastaveno globálně, ale ESET Endpoint Security se připojí k proxy serveru z důvodu aktualizace.
- Počítač je připojen k internetu pomocí proxy serveru. Nastavení bylo v průběhu instalace programu převzato z operačního systému, ale v průběhu času došlo ke změně nastavení proxy serveru (například z důvodu přechodu k jinému poskytovatel internetu). V tomto případě doporučujeme zkontrolovat nastavení proxy zobrazené v tomto okně a případně jej změnit pro zajištění funkčnosti aktualizací.

Standardně je nastavena možnost **Použít globální nastavení proxy serveru**.

Pokud aktivujete možnost **Použít přímé spojení, pokud není dostupný proxy server**, PRODUCTNAME automaticky zkusí připojení k aktualizačním serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.

Windows sdílení

Při stahování aktualizací ze složky z lokálního Windows serveru je pro vytvoření spojení standardně vyžadována autentifikace pomocí jména a hesla.

Pro konfiguraci účtu vyberte z rozbalovacího menu **Pro připojení do LAN vystupovat jako** jednu z následujících možností:

- **Systémový účet (standardně)**,
- **Aktuálně přihlášený uživatel**,
- **Definovaný uživatel**.

Po vybrání možnosti **Systémový účet (standardně)** se aplikace bude autentifikovat pod systémovým účtem. Za normálních okolností ověření neproběhne, pokud nejsou nastaveny autentifikační údaje v hlavním nastavení aktualizace.

Pokud vyberete tuto možnost, program se bude autentifikovat pod účtem **aktuálně přihlášeného uživatele**. Nevýhodou tohoto nastavení je nemožnost připojení na server a následné provedení aktualizace, pokud není na počítači přihlášen žádný uživatel.

Po vybrání této možnosti zadejte **přihlašovací údaje uživatele**, pod kterým se bude aplikace autentifikovat. Tuto možnost doporučujeme v případě, že se nezdaří připojení pod lokálním systémovým účtem. Uživatelský účet musí mít na lokálním serveru práva pro přístup do složky s aktualizačními soubory. V opačném případě se spojení nezdaří a aktualizace se nestáhne.

Uživatelské jméno a **heslo** jsou volitelné parametry.

> ⚠ Pokud vyberete možnost **Aktuálně přihlášený uživatel** nebo **Definovaný uživatel**, může nastat chyba při změně identity programu na požadovaného uživatele. Z tohoto důvodu doporučujeme u připojení do LAN nastavit autentifikační údaje v hlavním nastavení aktualizace. V tomto nastavení je potřeba uvést údaje ve tvaru *název_domény**uživatel* (případně pracovní skupiny: *název_pracovní_skupiny**uživatel*) a heslo. Při aktualizaci prostřednictvím HTTP lokálního serveru není standardně potřeba autentifikační údaje zadávat.

Po dokončení aktualizace **odpojit** ze serveru – pokud aktivujete tuto možnost, po dokončení aktualizace se vynutí ukončení spojení se serverem.

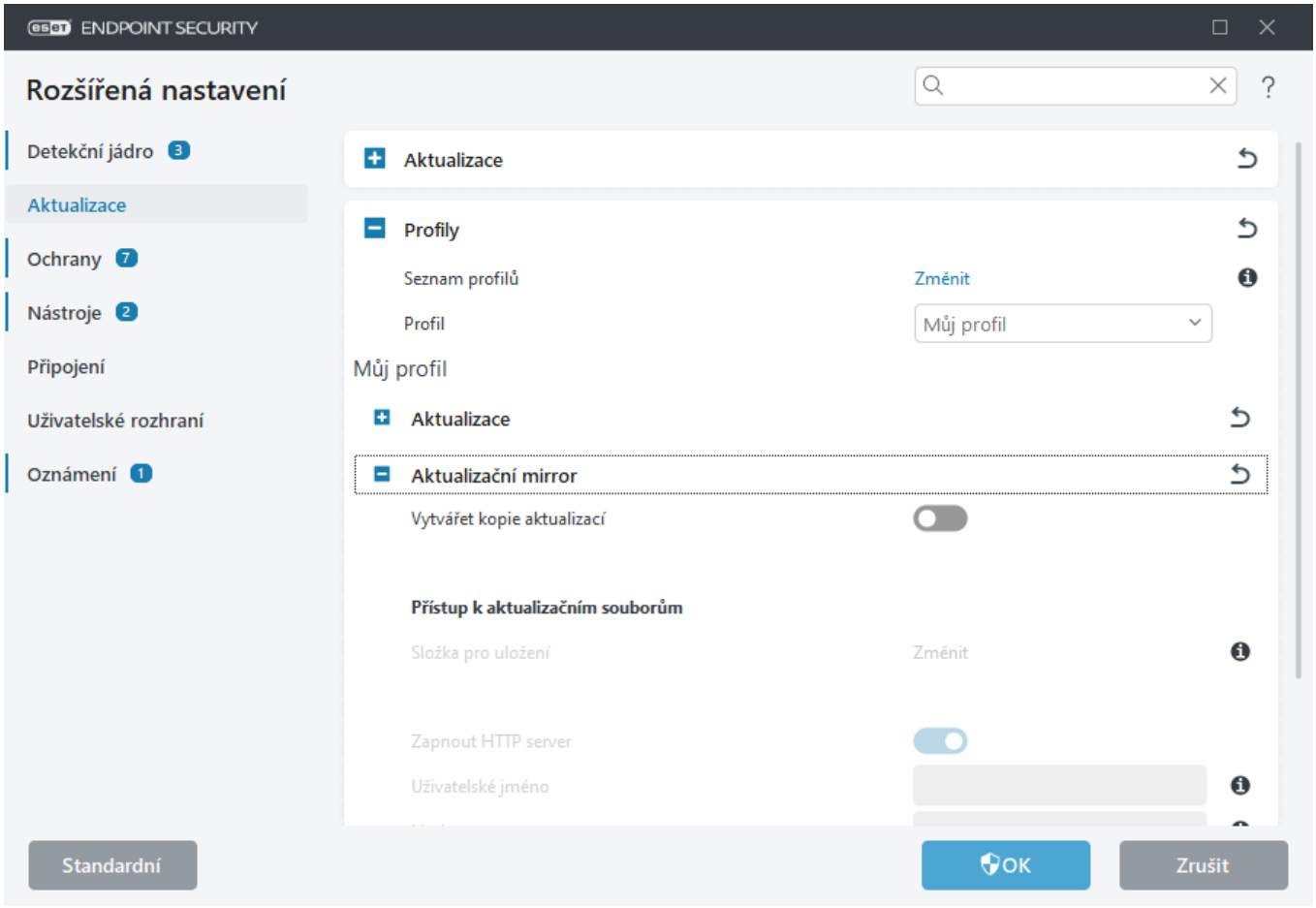
Mirror

ESET Endpoint Security umožňuje vytvářet kopie aktualizací, z níž lze pak aktualizovat další stanice v lokální síti. Vytváření kopií aktualizačních souboru je výhodné použít zejména ve velkých sítích, kde by aktualizace každé jedné stanice z Internetu způsobovala velký přenos dat a vytížení linek. Proto je doporučeno aktualizovat z internetu pouze jednoho klienta v síti a následně aktualizaci zpřístupnit pomocí tzv. mirroru (zrcadla) ostatním klientům v lokální síti. Aktualizace stanic z mirroru optimalizuje vyvážení zátěže sítě a šetří šířku pásma internetového připojení.

Aktualizační mirror produktu ESET Endpoint Security vytváří kopie aktualizací pouze pro stejnou generaci produktu na platformě Windows- Příklad: z mirroru vytvořeného produktem ESET Endpoint Security pro Windows ve verzi 10.x je možné aktualizovat pouze ESET Endpoint Antivirusa ESET Endpoint Security pro Windows ve verzi 10.x.

Ve velkých sítích, kde je pro správu používán ESET PROTECT, doporučujeme pro minimalizaci množství stahovaných dat z internetu upřednostnit ESET Bridge před konfigurací mirroru na některém z klientů. ESET Bridge můžete nainstalovat společně s ESET PROTECT prostřednictvím all-in-one instalačního balíčku nebo jej nasadit jako samostatnou komponentu. Pro více informací a přehled rozdílů mezi ESET Bridge, Apache HTTP Proxy, nástrojem Mirror Tool a přímým spojením přejděte do Online nápovědy k ESET PROTECT.

Možnosti konfigurace lokálního mirroru se nacházejí v části Rozšířená nastavení > **Aktualizace** > **Profily** > **Aktualizační mirror**.



Pro aktivaci funkce mirror vyberte v nastavení možnost **Vytvářet kopie aktualizací**. Zároveň tím zpřístupníte další nastavení mirroru jako je způsob přístupu k aktualizačním souborům a místo pro jejich uložení.

Přístup k aktualizačním souborům

Zapnout HTTP server – po aktivování začne program poskytovat aktualizační soubory pomocí interního HTTP serveru, kdy není nutné nastavovat uživatelské jméno a heslo pro autentifikaci.

Možnosti zpřístupnění mirroru jsou podrobněji vysvětleny v kapitole Způsoby zpřístupnění mirroru. Obecně existují dva základní způsoby zpřístupnění mirroru, a to buď prostřednictvím sdílené složky, nebo zpřístupněním aktualizací prostřednictvím interního HTTP serveru

Složku určenou pro ukládání aktualizačních souborů mirroru definujete v části **Složka pro uložení**. Pokud chcete

soubory ukládat do jiné složky, než je *C:\ProgramData\ESET\ESET Endpoint Security\mirror*, klikněte na **Vyčistit** a následně klikněte na **Změnit** a vyberte lokální nebo síťovou složku. Pokud je pro přístup do složky vyžadována autentifikace, musíte definovat **Uživatelské jméno** a **Heslo**. Pokud se požadovaná složka nachází na síťovém umístění, které pohání operační systém řady NT, musí mít uživatel, pod kterým se připojujete, oprávnění pro zápis do definovaného umístění. Uživatelské jméno zadávejte ve formátu *Doména/Uživatel* nebo *Pracovní skupina/Uživatel*. Nezapomeňte vyplnit heslo.

Mirror jako HTTP Server a dostupný prostřednictvím SSL

V sekci **HTTP Server** na záložce **Mirror** můžete definovat **Port serveru**, na kterém bude HTTP server naslouchat, stejně tak způsob **Autentifikace**. Standardně server naslouchá na portu **2221**.

Pomocí možnosti **Autentifikace** definujte režim autentifikace používaného pro přístup k aktualizačním souborům. K dispozici jsou následující možnosti: **Žádná**, **Základní**, **NTLM**. Vybráním možnosti **Základní** zajistíte, že uživatelské jméno a heslo bude šifrováno jednoduchou metodou kódování base64. Možnost **NTLM** zajistí bezpečné zakódování uživatelského jména a hesla. Pro autentifikaci se používají uživatelé vytvoření na stanici poskytující kopie aktualizací. Přednastavená možnost **Žádná** zpřístupní kopie aktualizací bez nutnosti autentifikace.

Autentifikační údaje, jako **Uživatelské jméno** a **Heslo**, slouží pro přístup k mirroru zprostředkovaného prostřednictvím HTTP serveru. Tato pole vyplňte pouze v případě, kdy jsou údaje vyžadovány.

Pro běh HTTP serveru s HTTPS (SSL) podporou vyberte vlastní **Soubor obsahující řetězec certifikátů** nebo vygenerujte certifikát podepsán sám sebou. K dispozici jsou následující **typy certifikátu**: ASN, PEM a PFX. Pro zvýšení bezpečnosti můžete použít zabezpečený HTTPS protokol pro poskytování kopií aktualizačních souborů. V takovém případě je téměř nemožné zjistit přenášená data a použité přístupové údaje. Jako **typ soukromého klíče** je standardně vybrána možnost **Integrovaný** (proto je možnost vybrat soubor obsahující **soukromý klíč** standardně nedostupná). To znamená to, že soukromý klíč je součástí souboru s řetězcem certifikátů.

Self-signed certifikát na HTTPS mirroru
Pokud na mirror serveru využijete HTTPS, bude nutné na všech stanicích, které se z něj mají aktualizovat, importovat tento certifikát do kořenového úložiště certifikátů. Pro více informací si v databázi znalostí společnosti Microsoft najděte článek Installing the trusted root certificate.

Aktualizace z mirroru

Existují dva základní způsoby zpřístupnění mirroru, který představuje repozitář pro klienty stahující si aktualizační soubory. Aktualizačními soubory se mohou nacházet ve sdílené složce nebo je lze zpřístupnit prostřednictvím HTTP serveru.

Aktualizační mirror produktu ESET Endpoint Security vytváří kopie aktualizací pouze pro stejnou generaci produktu na platformě Windows- Příklad: z mirroru vytvořeného produktem ESET Endpoint Security pro Windows ve verzi 10.x je možné aktualizovat pouze ESET Endpoint Antivirusa ESET Endpoint Security pro Windows ve verzi 10.x.

Zpřístupnění mirroru prostřednictvím lokálního HTTP serveru

Je použito automaticky jako předdefinované nastavení, při standardní instalaci. Proto pro zpřístupnění mirroru pomocí HTTP serveru otevřete Rozšířená nastavení >**Aktualizace** > **Profily** > **Aktualizační mirror** a aktivujte možnost **Vytvářet kopie aktualizací**.

V sekci **HTTP Server** na záložce **Mirror** můžete definovat **Port serveru**, na kterém bude HTTP server naslouchat, stejně tak způsob **Autentifikace**. Standardně server naslouchá na portu **2221**.

Pomocí možnosti **Autentifikace** definujte režim autentifikace používaného pro přístup k aktualizačním souborům. K dispozici jsou následující možnosti: **Žádná**, **Základní**, **NTLM**. Vybráním možnosti **Základní** zajistíte, že uživatelské jméno a heslo bude šifrováno jednoduchou metodou kódování base64. Možnost **NTLM** zajistí bezpečné zakódování uživatelského jména a hesla. Pro autentifikaci se používají uživatelé vytvoření na stanici poskytující kopie aktualizací. Přednastavená možnost **Žádná** zpřístupní kopie aktualizací bez nutnosti autentifikace.

Při této metodě zpřístupnění mirroru musí být složka mirroru na stejném počítači, na kterém je ESET Endpoint Security nainstalován.

Po několika neúspěšných pokusech o aktualizaci z mirroru se v hlavním okně programu na záložce Aktualizace zobrazí chyba **Neplatné uživatelské jméno nebo heslo**. V takovém případě otevřete Rozšířená nastavení > **Aktualizace** > **Profily**> **Aktualizační mirror** a ověřte zadané uživatelské jméno a heslo. Nejčastějším důvodem pro zobrazení této chyby jsou chybně zadané přihlašovací údaje.

Po dokončení nastavení mirroru je potřeba na klientských stanicích nastavit nový aktualizační server. Tuto operaci provedete pomocí následujících kroků:

- Otevřete Rozšířená nastavení a klikněte na **Aktualizace** > **Profily** > **Aktualizace** > **Aktualizace modulů**.
- Deaktivujte možnost **Automatický výběr serveru** a do pole **Vlastní server** zadejte adresu nového serveru v jednom z následujících formátů:
  http://IP_adresa_serveru:2221
  https://IP_adresa_serveru:2221 (pokud je použito SSL)

Zpřístupnění mirroru prostřednictvím síťového sdílení

Nejprve je nutné na lokálním nebo síťovém zařízení vytvořit sdílenou složku. Při jejím vytváření musíte nastavit práva pro zápis do této složky uživateli, který bude kopie aktualizací do této složky ukládat, nastavit práva pro čtení uživateli, který si aktualizace z této složky stahovat (aktualizovat ESET Endpoint Security).

Následně v rozšířeném nastavení (F5) v sekci **Aktualizace** > **Profily** > **Aktualizační mirror** deaktivujte možnost **Zapnout HTTP serveru**. Tato možnost je ve výchozí konfiguraci zapnutá.

V případě umístění sdílené složky na jiném počítači v síti je nutné zadat přístupové údaje k tomuto počítači. Uživatelské jméno a heslo zadejte v Rozšířeném nastavení v sekci **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení** > **Windows sdílení** > **Pro připojení do LAN vystupovat jako**. Jedná o stejné nastavení používané při aktualizace a je popsané v kapitole Pro připojení do LAN vystupovat jako.

Pro přístup ke složce s mirrorem je nutné přistupovat pod uživatelským účtem, pod kterým je možné se přihlásit na počítač, na kterém je mirror vytvořen. V doménovém prostředí použijte přihlašovací údaje ve formátu "doména\uživatel". V případě ne-doménových prostředí "IP_adresa_stanice\uživatel" nebo "název_stanice\uživatel".

Po dokončení nastavení mirroru je potřeba na klientských stanicích nastavit nový aktualizační server (cestu k *UNC**PATH*). Tuto operaci provedete pomocí následujících kroků:

1. Otevřete Rozšířená nastavení produktu a přejděte do sekce **Aktualizace** > **Profily** > **Aktualizace**.
2. V části **Aktualizace modulů** deaktivujte možnost **Automatický výběr serveru** a do pole **Vlastní server** zadejte adresu v následujícím formátu: *UNC**CESTA*.

Při zadávání cesty k aktualizačnímu serveru je důležité cestu specifikovat v UNC formátu. Aktualizace z namapovaných disků nemusí fungovat správně.

Vytvoření mirroru prostřednictvím Mirror Toolu
Mirror tool vytváří, ve srovnání s funkcí mirror v produktu, odlišnou adresářovou strukturu. V každé složce se nachází soubory pro konkrétní skupinu produktů. Je tedy nutné v nastavení aktualizace definovat správnou cestu.
Příklad: pro aktualizaci ESET PROTECT z mirroru zadejte do pole Aktualizační server hodnotu (dle umístění kořene svého HTTP serveru):
`http://your_server_address/mirror/eset_upd/ep10`

Poslední sekce se týká aktualizace programových komponent (PCU). Standardně jsou programové komponenty stahovány a automaticky umísťovány do složky s mirrorem. Pokud je aktivní možnost **Aktualizace programu**, není nutné kliknout na tlačítko **Aktualizovat**, protože jsou automaticky umisťovány do složky s mirrorem ve chvíli, kdy jsou dostupné. Pro více informací o aktualizaci produktu přejděte do kapitoly Režim aktualizace.

Řešení problémů při aktualizaci z mirroru

Ve většině případů jsou problémy při aktualizaci z mirroru způsobovány jedním z následujících důvodů: špatná konfigurace Mirroru, neplatné autentifikační údaje pro přístup ke složce s mirrorem, chybně nastavená stanice, která má stahovat aktualizační soubory z mirroru nebo kombinace uvedených důvodů. Níže přidáváme přehled nejčastějších problémů, které mohou nastat při aktualizaci z mirroru:

ESET Endpoint Security nenaváže spojení s mirrorem – pravděpodobně způsobeno nesprávným zadáním aktualizačního serveru (sítové cesty ke složce s mirrorem), ze kterého se má stanice aktualizovat. Správnost zadané cesty ověřte stisknutím kláves **Win + R** (případně klikněte na tlačítko **Start** > Spustit) a zadáním uvedené cesty k mirroru. Pokud je cesta zadána správně, po kliknutí na tlačítko OK by se měl zobrazit obsah složky s mirrorem.

ESET Endpoint Security vyžaduje zadání uživatelského jména a hesla – pravděpodobně způsobeno nesprávným zadáním autentifikačních údajů (uživatelského jména a hesla) v nastavení aktualizace. Jedná se o uživatelské jméno a heslo, pod kterým program přistupuje k aktualizačnímu serveru, ze kterého se má aktualizovat. Ujistěte se, že jsou autentizační údaje správné a zadané ve správném formátu. Například název_domény\uživatel nebo název_pracovni_skupiny\uživatel a heslo. Pokud je složka s mirrorem zpřístupněna pro "Everyone" (tj. anglicky, pro "každého"), je potřeba toto uživatelské oprávnění brát s rezervou. "Everyone" neznamená jakýkoli neověřený uživatel, ale znamená to pouze, že složka je přístupná pro všechny uživatele dané domény. I když je tedy složka s mirrorem přístupná pro "Everyone", v nastavení aktualizace je stále potřeba zadat přihlašovací údaje konkrétního uživatele.

ESET Endpoint Security nenaváže spojení k mirroru – není povolena komunikace na portu, na kterém běží HTTP server.

ESET Endpoint Security zahlásí chybu při stahování aktualizačních souborů – nejčastěji jde o chybnou konfiguraci aktualizačního serveru (síťové cesty ke složce s mirrorem).

Ochrany

Ochrany chrání systém před útoky škodlivého kódu tím, že kontroluje komunikaci se soubory, e-maily a internetem. Například pokud je detekován objekt klasifikovaný jako malware, zahájí se akce pro řešení situace. Škodlivý kód může být zablokován a následně léčen, odstraněn nebo přesunut do karantény.

Chcete-li podrobně nakonfigurovat ochrany, otevřete Rozšířená nastavení > **Ochrany**.

Změny v Ochranách by měl provádět pouze zkušený uživatel. Chybnou úpravou nastavení se může snížit úroveň ochrany.

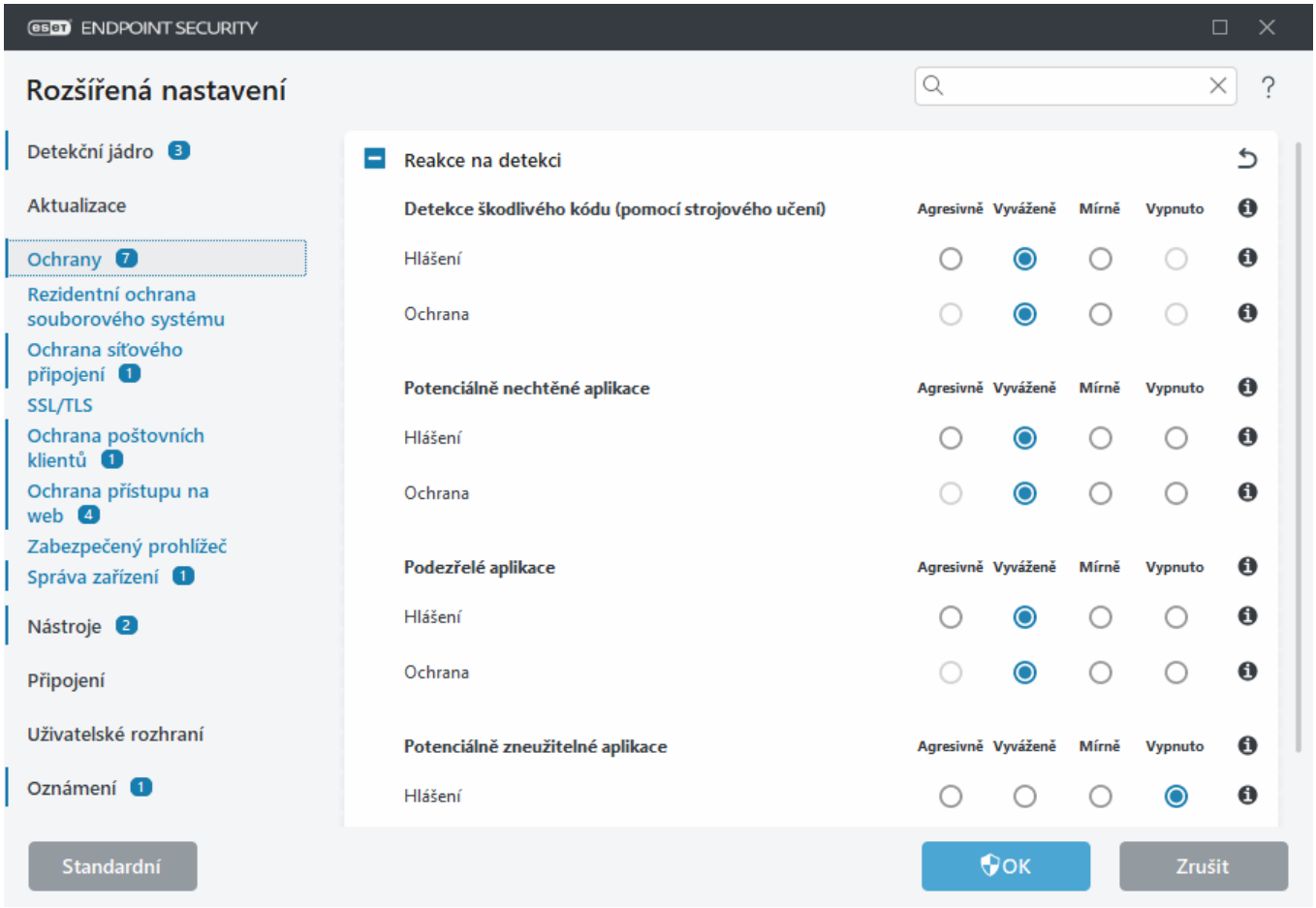
V této kapitole naleznete:

Reakce na detekci

Reakce na detekci umožňují nastavit úrovně hlášení a ochrany pro následující kategorie:

- **Detekce škodlivého kódu (pomocí strojového učení)** – počítačový virus je část škodlivého kódu, která je připojena k existujícím souborům v počítači. Termín "virus" bývá často vykládán nesprávně. Vhodnějším výrazem je "malware" (škodlivý software). Detekce malwaru zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Více informací o tomto typu aplikací naleznete ve slovníku pojmů.

- **Potenciálně nechtěné aplikace** – grayware (neboli PUA – potentially unwanted aplication) představují širokou škálu aplikací, které nejsou jednoznačně škodlivé jako viry nebo trojské koně. Mohou však instalovat nechtěný software, měnit chování vašeho zařízení, provádět neočekávané operace, případně akce bez vědomí uživatele. Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- Mezi **potenciálně podezřelé aplikace** řadíme rovněž programy, které jsou komprimovány pomocí packerů nebo protektorů Tuto metodu často využívající tvůrci škodlivého kódu, aby se vyhnuli detekci ze strany antiviru.
- **Potenciálně zneužitelné aplikace** – legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti. Příkladem mohou být programy pro vzdálené připojení, aplikace k odšifrování hesel a keyloggery (programy, které zaznamenávají uživatelem zadané znaky na klávesnici). Více informací o tomto typu aplikací naleznete ve slovníku pojmů.



Vylepšená ochrana

Pokročilé strojové učení je nyní funguje jako pokročilá vrstva ochrany a vylepšuje tak detekci. Pro více informací o tomto typu ochranu se podívejte do slovníku pojmů.

Nastavení hlášení

Při výskytu detekce (například při objevení hrozby klasifikované jako malware) se informace zapíše do Detekčního protokolu a může se zobrazit Oznámení na pracovní ploše (pokud je to v produktu ESET Endpoint Security povoleno).

Práh (úroveň) hlášení můžete konfigurovat jednotlivě pro každou kategorii (dále jen "KATEGORIE"):

1. Detekce škodlivého kódu
2. Potenciálně nechtěné aplikace
3. Potenciálně zneužitelné aplikace
4. Podezřelé aplikace

Hlášení zajišťuje detekční jádro včetně komponenty strojového učení. Pro hlášení můžete nastavit vyšší práh, než je aktuální úroveň ochrany. Tato nastavení nemají vliv na blokování, léčení nebo odstraňování objektů.

Před změnou prahu (úrovně) pro danou KATEGORII si přečtěte níže uvedené informace:

Práh	Vysvětlení
Agresivně	Hlášení z dané KATEGORIE je nakonfigurováno na nejvyšší citlivost. Hlášeno bude větší množství detekcí. V **agresivním** nastavení může docházet k chybné identifikaci některých objektů patřících do KATEGORIE.
Vyváženě	Hlášení z dané KATEGORIE je nakonfigurováno jako vyvážené. Toto nastavení je optimalizováno s ohledem na výkon, přesnost detekce a množství falešných poplachů.
Mírně	Hlášení z dané KATEGORIE je nakonfigurováno tak, aby se minimalizoval počet falešných poplachů při zachování dostatečné úrovně zabezpečení. Objekty budou hlášeny pouze v případě vysoké pravděpodobnosti a shody chování odpovídající KATEGORII.
Vypnuto	Hlášení pro danou KATEGORII není aktivní a detekce tohoto typu nebudou zachytávány, hlášeny ani léčeny. V důsledku tohoto nastavení bude vypnuta ochrana před tímto typem detekce. V rámci hlášení malwaru není k dispozici možnost Vypnuto. Tato hodnota je výchozí pro potenciálně zneužitelné aplikace.

Dostupnost modulů ochrany produktu ESET Endpoint Security

Níže uvádíme dostupnost jednotlivých prahů KATEGORIÍ (zapnuto nebo vypnuto) v modulech ochrany:

	Agresivně	Vyváženě	Mírně	Vypnuto*
Modul pokročilého strojového učení	✔ (agresivní režim)	✔ (konzervativní režim)	X	X
Modul detekčního jádra	✔	✔	✔	X
Ostatní moduly ochrany	✔	✔	✔	X

** Nedoporučeno.

Jak zjistím verzi produktu, programových modulů a data sestavení?

1. V hlavním okně programu klikněte na **Nápověda a podpora** > **O programu ESET Endpoint Security**.
2. V zobrazeném dialogovém okně **O programu** se na prvním řádku zobrazuje číslo verze vámi používaného produktu ESET.
3. Pro zobrazení informací o jednotlivých modulech klikněte na tlačítko **Nainstalované programové komponenty**.

Důležité poznámky

Při konfiguraci vhodných prahů ve svém prostředí vezměte v potaz následující informace:

- Možnost **Vyváženě** je doporučená pro většinu situací.
- Možnost **Mírně** je doporučená pro prostředí, kdy je prioritou minimalizace počtu falešných detekcí způsobených bezpečnostním softwarem.
- Čím vyšší práh nastavíte, tím vyšší bude počet detekcí. Zároveň se zvedne pravděpodobnost výskytu falešně detekovaných objektů.
- Z pohledu reálného světa není možné zaručit 100% úspěšnost detekce, stejně tak nulovou pravděpodobnost, že bude čistý objekt označen jako malware.
- Pro zajištění maximální rovnováhy mezi výkonem, přesností detekce a počtem falešně detekovaných objektů udržuje ESET Endpoint Security a jeho moduly aktuální.

Nastavení ochrany

Pokud je detekovaný objekt klasifikován jako KATEGORIE, program jej zablokuje, a následně vyléčí, odstraní nebo přesune do karantény.

Před změnou prahu (úrovně) pro danou KATEGORII si přečtěte níže uvedené informace:

Práh	Vysvětlení
Agresivně	Detekce zachycené s úrovní Agresivně (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení). Toto nastavení je doporučeno, pokud na všech koncových zařízeních proběhla kontrola s agresivním nastavením a chybně detekované objekty jste přidali do detekčních výjimek.
Vyváženě	Detekce zachycené s úrovní Vyváženě (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Mírně	Detekce zachycené s úrovní Opatrně jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Vypnuto	Toto nastavení je užitečné pro identifikaci a vytvoření výjimek na falešně detekované objekty. V rámci ochrany před malwarem není k dispozici možnost Vypnuto. Tato hodnota je výchozí pro potenciálně zneužitelné aplikace.

Osvědčené postupy

NESPRAVOVANÉ PROSTŘEDÍ (jednotlivé stanice)

Doporučujeme konfiguraci ponechat tak, jak je.

SPRAVOVANÉ PROSTŘEDÍ

Tato nastavení se zpravidla aplikují prostřednictvím politik.

1. Prvotní fáze

Tato fáze může trvat až týden.

- Práh **hlášení** nastavte na úroveň **Vyváženě**.
  POZNÁMKA: Pokud to vyžadujete, nastavte úroveň **Agresivně**.
- Nastavte nebo ponechte práh **ochrany** pro škodlivý kód na úrovni **Vyváženě**.
- Pro ostatní KATEGORIE nastavte práh **ochrany** na úroveň **Mírně**.
  POZNÁMKA: V této fázi nedoporučujeme nastavit práh **ochrany** na úroveň **Agresivně**. Došlo by totiž k vyléčení všech nalezených detekcí, včetně falešně identifikovaných.
- V detekčních protokolu najděte falešně identifikované objekty a vytvořte pro ně detekční výjimky.

2. Přechodná fáze

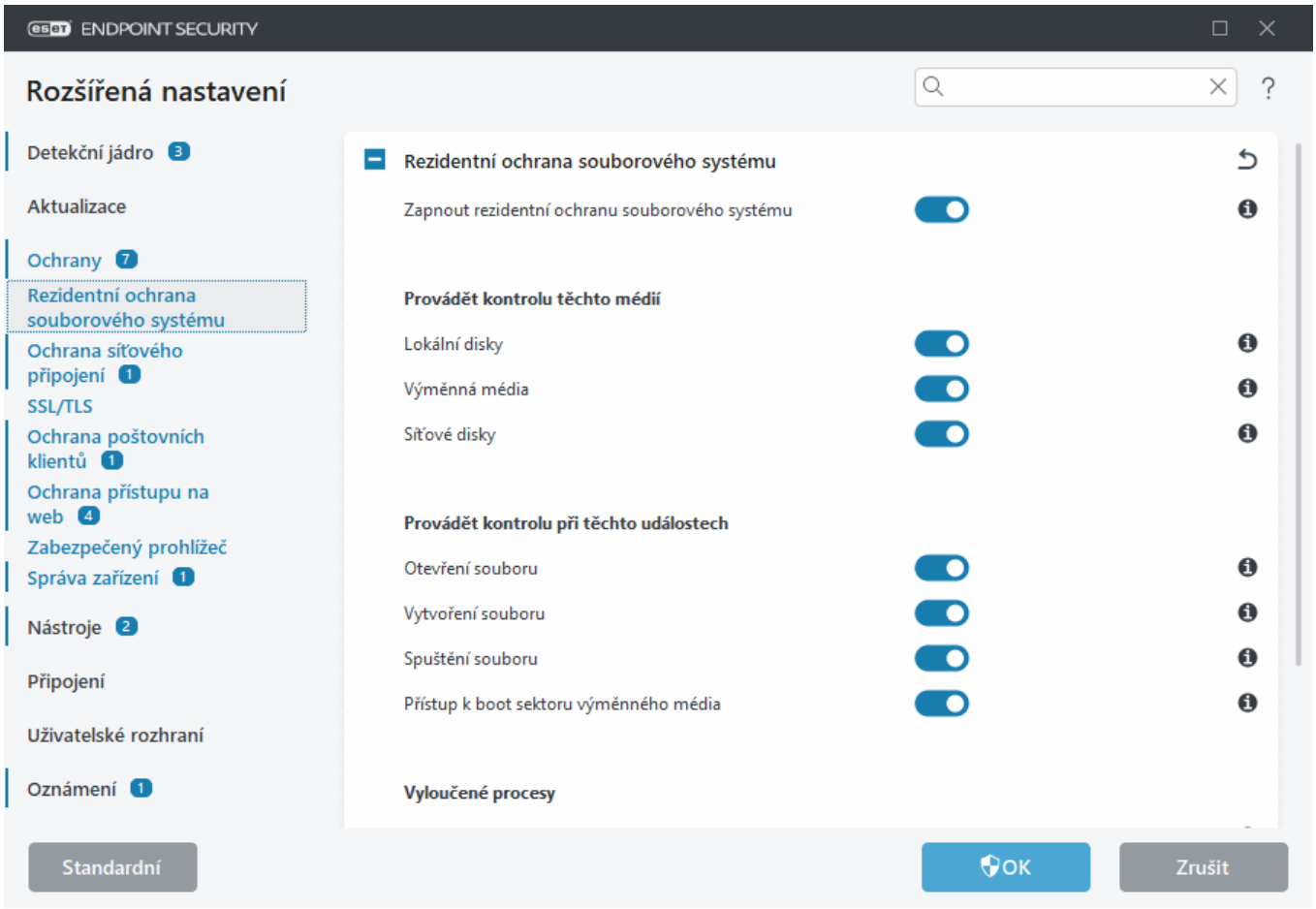
- "Produkční fázi" nejprve v rámci testování implementujte na vybrané stanice (nikoli na všechny stanice v síti).

3. Produkční fáze

- Práh **ochrany** nastavte na úroveň **Vyváženě**.
- Případně můžete využít předdefinovanou politiku pro ESET Endpoint Security.
- **Agresivní** práh ochrany nastavte v případě, že vyžadujete nejvyšší míru detekci a akceptujete výskyt falešně identifikovaných objektů.
- Zkontrolujte detekční protokol, případně chybějící detekce hledejte v ESET PROTECT.

Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému vyhledává škodlivý kód ve všech souborech v systému, které se otevírají, vytvářejí nebo spouštějí.



Standardně se rezidentní ochrana spustí vždy při startu operačního systému. Nedoporučujeme vypínat **Zapnout rezidentní ochranu souborového systému** v Rozšířeném nastavení > **Ochrany** > **Rezidentní ochrana souborového systému**.

Kontrola médií

Standardně je nastavena kontrola všech typů médií:

- **Lokální disky** – kontroluje všechny systémové a lokální pevné disky (například *C:*\, *D:*\).
- **Výměnná média** – kontroluje CD, DVD, USB úložiště, paměťové karty, atp.

- **Síťové disky** – kontroluje všechny namapované síťové jednotky (například kdy pod písmenem *H:*\ máte *store04*), stejně tak síťová umístění přímo (například *store08*).

Doporučujeme ponechat toto nastavení. Změnu doporučujeme pouze ve zvláštních případech, např. pokud při kontrole určitého média dochází k výraznému zpomalení.

Kontrola při událostech

Standardně jsou kontrolovány všechny soubory, jakmile jsou otevřené, vytvořené nebo spuštěné. Tato nastavení doporučujeme ponechat pro zajištění maximální možné ochrany počítače:

- **Otevření souboru** – zapne/vypne kontrolu otevíraných souborů.
- **Vytvoření souboru** – zapne/vypne kontrolu vytvářených nebo modifikovaných souborů.
- **Spuštění souboru** – zapne/vypne kontrolu spouštěných souborů.
- **Přístup na boot sektor výměnného zařízení** – pokud obsahuje vložené výměnné médium boot sektor, po připojení média do zařízení dojde automaticky ke kontrole sektoru. Tato možnost nezapíná kontrolu souborů na výměnných médiích. Nastavení kontroly na výměnných médiích se nachází v části **Provádět kontrolu těchto médií** > **Výměnná média**. Aby **kontrola boot sektoru výměnných médií** fungovala správně, ponechte v ThreatSense zapnutou funkci **Boot sektory/UEFI**.

Vyloučené procesy

Viz Vyloučené procesy.

ThreatSense

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí jako je přístup k souboru. Při kontrole jsou používány detekční metody technologie **ThreatSense** (ty jsou popsány v kapitole Nastavení skenovacího jádra ThreatSense). Chování rezidentní ochrany souborového systému lze nakonfigurovat tak, aby se s nově vytvořenými soubory zacházelo jinak než s existujícími soubory. Například, pro nově vytvářené soubory můžete nastavit hlubší úroveň kontroly.

Pro zajištění minimálních systémových nároků, nejsou již dříve kontrolované soubory znovu kontrolovány (pokud nebyly změněny). Soubory jsou opět kontrolovány pouze po každé aktualizaci detekčních modulů. Toto chování můžete přizpůsobit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje. Chcete-li toto nastavení upravit, otevřete Rozšířená nastavení > **Ochrany** > **Rezidentní ochrana souborového systému**. Klikněte na **ThreatSense** > **Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

Rezidentní ochrana souborového systému také umožňuje konfigurovat Další parametry ThreatSense.

Vyloučené procesy

Pomocí této funkce vyloučíte z Rezidentní ochrany souborového systému činnost konkrétních procesů. V případě obnovy dedikovaných serverů (aplikačních, souborových atd.) ze zálohy do funkčního stavu hraje kritickou roli čas. Při navýšení rychlosti zálohování, zajištění integrity dat a dostupnosti služeb jsou některá zálohovací řešení technicky v konfliktu s antivirovou ochranou souborového systému. Jediným řešením pro zabránění konfliktu bývá deaktivace anti-malware řešení. Vyloučením činnosti konkrétních procesů (například zálohovacího agenta) z kontroly je veškerá jejich činnost ignorována a považována za důvěryhodnou, čímž je minimalizován vliv na celý

průběh operace (například zálohování). Při vytváření výjimek však buďte obezřetní. Při přístupu zálohovacího agenta k infikovanému souboru nedojde k detekci a hlášení hrozby. Z tohoto důvodu je možné výjimky vytvářet pouze z rezidentní ochrany souborového systému.

Nezaměňujte tuto funkci s možností pro vyloučení přípon souborů z kontroly, tvorbu HIPS výjimek, detekčních výjimek nebo výkonnostních výjimek.

Prostřednictvím těchto výjimek můžete minimalizovat možné konflikty a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (*.exe*).

Spustitelné soubory můžete přidat do seznamu vyloučených procesů v Rozšířeném nastavení > **Ochrany** > **Rezidentní ochrana souborového systému** > **Rezidentní ochrana souborového systému** > **Vyloučené procesy**.

Tato funkce byla navržena pro vytvoření výjimek na zálohovací nástroje. Vyloučením zálohovacích nástrojů z kontroly nemá pouze vliv na stabilitu systému, ale také rychlost zálohování.

Kliknutím na **Změnit** si otevřete správce **Výjimek**, kde pomocí tlačítka Přidat a použitím průzkumníka vyberete spustitelný soubor (například *Backup-tool.exe*), který chcete vyloučit z kontroly.
Po přidání *.exe* souboru na seznam výjimek přestane ESET Endpoint Security monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

Pokud pro výběr procesu nevyužijete průzkumníka, zadejte absolutní cestu k procesu manuálně. V opačném případě nebude výjimka fungovat korektně a HIPS může generovat chyby.

Seznam procesů vyloučených z kontroly můžete kdykoli **upravit**, stejně tak proces ze seznamu výjimek **odstranit**.

Pro vyloučené procesy se vytvoří výjimka pouze v rezidentní ochraně souborového systému. Pokud například vyloučíte spustitelný soubor internetového prohlížeče, soubory stahované z internetu budou nadále kontrolovány Ochranou přístupu na web. Tím je zajištěno, že hrozba, která se snaží dostat do počítače touto cestou, bude detekována. Jedná se pouze o příklad. Z bezpečnostních důvodů nedoporučujeme vytvářet výjimku na internetový prohlížeč.

Přidání a úprava výjimek pro procesy

Kliknutím na tlačítko **Přidat** můžete v tomto dialogovém okně vytvořit v detekčním jádře výjimku na činnost procesu. Prostřednictvím těchto výjimek můžete minimalizovat možné konflikty a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (*.exe*).

Kliknutím na … vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace.
Po přidání *.exe* souboru na seznam výjimek přestane ESET Endpoint Security monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

Pokud pro výběr procesu nevyužijete průzkumníka, zadejte absolutní cestu k procesu manuálně. V opačném případě nebude výjimka fungovat korektně a HIPS může generovat chyby.

Seznam procesů vyloučených z kontroly můžete kdykoli **upravit**, stejně tak proces ze seznamu výjimek **odstranit**.

Kdy měnit nastavení rezidentní ochrany

Rezidentní ochrana je klíčovým modulem zabezpečujícím ochranu počítače. Proto je potřeba být při změnách nastavení obezřetný. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech.

Po instalaci ESET Endpoint Security jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Chcete-li obnovit výchozí nastavení, klikněte na ↩ vedle položky v Rozšířených nastaveních > **Ochrany** > **Reakce na detekci**.

Ověření funkčnosti rezidentní ochrany

Pro ověření funkčnosti rezidentní ochrany použijte testovací soubor eicar.com. Tento soubor je speciální neškodný objekt, který detekují všechny antivirové programy. Soubor vyvinula společnost EICAR (European Institute for Computer Antivirus Research) za účelem testování antivirových programů.

Soubor eicar je dostupný na adrese http://www.eicar.org/download/eicar.com.
Po zadání této URL adresy do prohlížeče by se měla objevit zpráva, že hrozba byla odstraněna.

Co dělat, když nefunguje rezidentní ochrana

V této části popisujeme problémové stavy, které mohou nastat při běhu rezidentní ochrany. Je zde také uvedeno jak postupovat při jejich řešení.

Rezidentní ochrana je vypnutá

Pokud uživatel nechtěně zakáže rezidentní ochranu, měli byste funkci znovu aktivovat. Chcete-li znovu aktivovat rezidentní ochranu, přejděte v hlavním okně programu do nabídky **Nastavení** a klikněte na položku **Počítač** > **Rezidentní ochrana souborového systému**.

Pokud se rezidentní ochrana nespouští při startu operačního systému, pravděpodobně byla vypnuta možnost **Zapnout rezidentní ochranu souborového systému**. Chcete-li se ujistit, že je tato možnost povolena, otevřete Rozšířená nastavení > **Ochrany** > **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

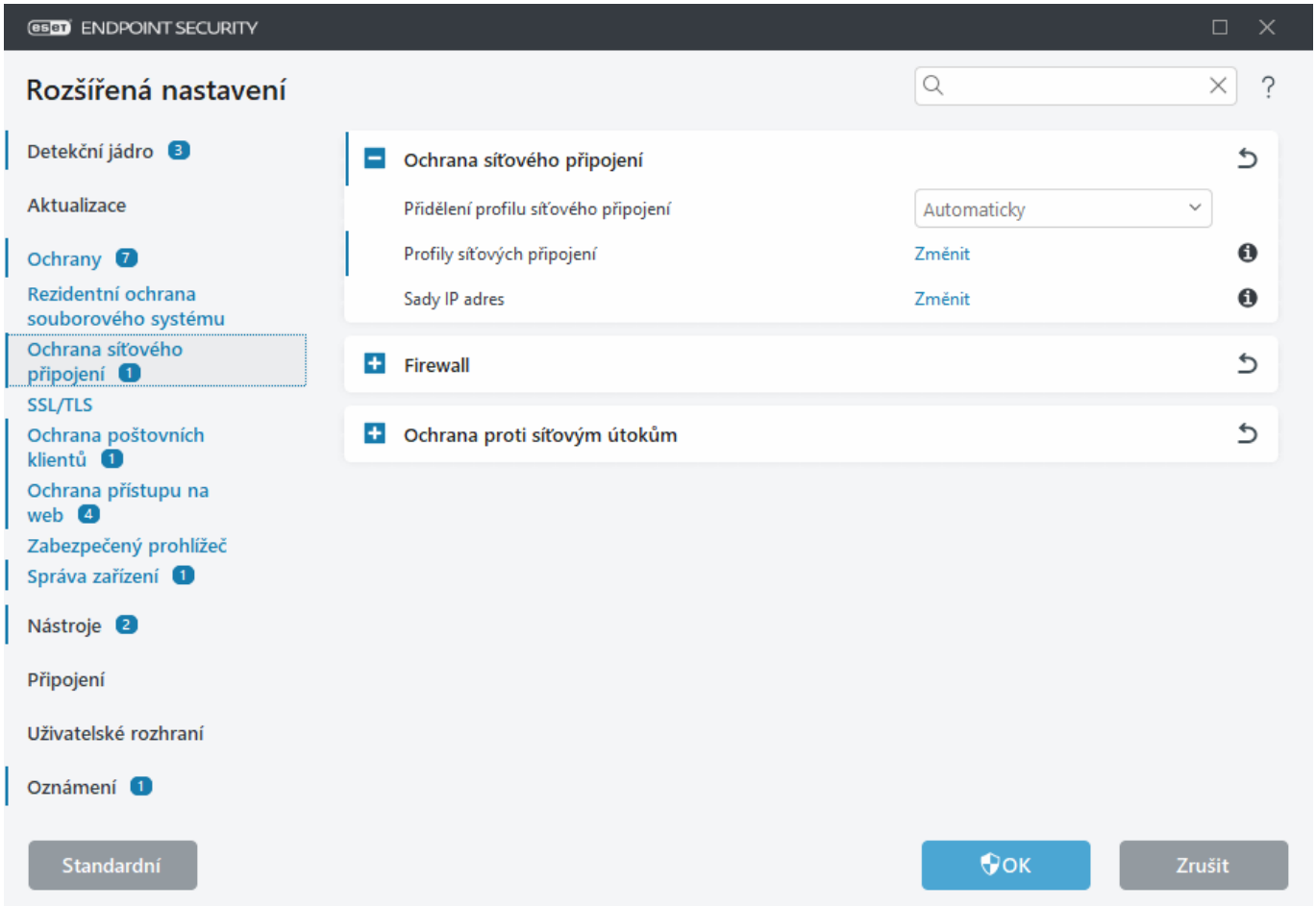
Ujistěte se, zda nemáte nainstalován další antivirový program. Pokud jsou na zařízení nainstalované dva bezpečnostními programy, může mezi nimi docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Zapnout rezidentní ochranu souborového systému**, zřejmě dochází ke konfliktu s jiným programem. Pokud chcete problém vyřešit, vytvořte ESET SysInspector protokol a odešlete jej k analýze technické podpoře ESET.

Ochrana síťového připojení

Ochrana síťového připojení umožňuje konfigurovat všechna síťová připojení. Na základě konfigurace můžete povolit/zakázat přístup k počítači v určitých sítích, povolit/zakázat přístup k síťovým zařízením z počítače a další. Ve výchozím nastavení má ESET Endpoint Security pravidla firewallu a ochranu síťového připojení předem nakonfigurované pro maximální zabezpečení. Ve specifických prostředích však může být nutná vlastní konfigurace. Změnu výchozího nastavení by měl provádět pouze zkušený uživatel.



Následující nastavení můžete nakonfigurovat v části Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** (podrobný popis jednotlivých možností ochrany síťového připojení naleznete po kliknutí na níže uvedené odkazy):

Ochrana síťového připojení

Profily síťových připojení – profily lze použít k řízení Ochrany síťového připojení a Firewallu pro konkrétní síťová připojení.

Sady IP adres – můžete definovat kolekce IP adres, které vytvářejí jednu logickou skupinu IP adres, kterou pak lze použít pro pravidla Firewallu a Ochranu proti útokům hrubou silou.

Firewall

Ochrana proti síťovým útokům

Profily síťových připojení

Profily lze použít k řízení chování Ochrany síťového připojení ESET Endpoint Security pro konkrétní Síťové připojení. Když v programu vytváříte nebo upravujete pravidla firewallu, IDS pravidla nebo pravidla Ochrany proti útokům hrubou silou, můžete je přiřadit konkrétnímu profilu nebo je použít pro všechny profily. Pokud je profil v síťovém připojení aktivní, jsou na něj aplikována pouze globální pravidla (pravidla bez zadaného profilu) a pravidla, která byla tomuto profilu přiřazena. Můžete vytvořit více profilů s různými pravidly přiřazenými síťovým připojením a snadno tak změnit chování firewallu.

Profily a přiřazení síťových připojení můžete konfigurovat v Rozšířeném nastavení > **Ochrany** > **Ochrana síťového připojení** > **Ochrana síťového připojení**.

Přidělení profilu síťového připojení – umožňuje zvolit, zda má být nově zjištěným síťovým připojením automaticky (v rozbalovacím menu vyberte možnost **Auto**) přiřazen předdefinovaný nebo vlastní profil na základě Spouštěčů nakonfigurovaných v profilech síťových připojení, nebo zda chcete být při zjištění nového síťového připojení vyzváni (v rozevírací nabídce vyberte možnost **Dotázat se**) ke konfiguraci ochrany sítě a přiřazení profilu ručně.

Konkrétní profil síťového připojení můžete přiřadit také ručně v hlavním okně programu > **Nastavení** > **Síť** > **Připojené sítě**. Najeďte na konkrétní síťové připojení a kliknutím na ikonu nabídky ⋮ > **Změnit** otevřete okno Nastavení ochrany sítě a vyberte profil.

Profily síťového připojení – kliknutím na **Změnit** přidáte nebo upravíte profily síťového připojení.

Následující profily jsou předdefinované a nelze je upravovat nebo odstraňovat:

Privátní – pro důvěryhodné sítě (domácí nebo firemní síť). Vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti (přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít v bezpečných lokálních sítích. Tento profil je automaticky přiřazen síťovému připojení, pokud je nakonfigurováno jako doménová nebo privátní síť ve Windows.

Veřejná – pro nedůvěryhodné sítě (veřejná síť). Soubory a složky uložené ve vašem počítači nebudou pro ostatní uživatele v síti dostupné, stejně tak nebude počítač viditelný v síti. Sdílení systémových prostředků bude deaktivováno. Toto nastavení doporučujeme při připojení k bezdrátovým sítích. Tento profil je automaticky přiřazen každému síťovému připojení, které není nakonfigurováno jako doménová nebo privátní síť ve Windows.

Po přepnutí síťového připojení na jiný profil se v pravém dolním rohu obrazovky zobrazí oznámení.

Přidání nebo úprava profilů síťového připojení

Profily síťového připojení můžete přidat nebo upravit v Rozšířených nastaveních > **Ochrany** > **Ochrana síťového připojení** > **Ochrana síťového připojeni** > **Profily síťových připojení** > **Změnit**. Chcete-li profil upravit, musíte jej vybrat ze seznamu **Profilů síťových připojení**.

Následující profily jsou předdefinované a nelze je upravovat nebo odstraňovat:

Privátní – pro důvěryhodné sítě (domácí nebo firemní síť). Vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti

(přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít v bezpečných lokálních sítích. Tento profil je automaticky přiřazen síťovému připojení, pokud je nakonfigurováno jako doménová nebo privátní síť ve Windows.

Veřejná – pro nedůvěryhodné sítě (veřejná síť). Soubory a složky uložené ve vašem počítači nebudou pro ostatní uživatele v síti dostupné, stejně tak nebude počítač viditelný v síti. Sdílení systémových prostředků bude deaktivováno. Toto nastavení doporučujeme při připojení k bezdrátovým sítích. Tento profil je automaticky přiřazen každému síťovému připojení, které není nakonfigurováno jako doménová nebo privátní síť ve Windows.

Tlačítka **Nahoru/Výše/Níže/Dolů**  – umožňují nastavit úroveň priority profilů síťového připojení (profily síťového připojení jsou vyhodnoceny a použity podle své priority. Vždy se použije první odpovídající profil).

Přidání nebo úprava profilu

Vlastní profil síťového připojení umožňuje použít Pravidla firewallu, pravidla Ochrany před útoky hrubou silou a provádět další nastavení pro konkrétní síťová připojení. V sekci Spouštěče určíte, ke kterým síťovým připojením bude vlastní profil přiřazen.

Chcete-li otevřít editor profilů v okně **Profily síťových připojení**:

- Klikněte na **Přidat**.
- Vyberte jeden z existujících profilů a klikněte na tlačítko **Změnit**.
- Vyberte jeden z existujících profilů a klikněte na tlačítko **Kopírovat**.

Název – název vlastního profilu.

Popis – popis profilu, který pomáhá profil identifikovat.

Vždy důvěryhodné adresy – zde definované adresy jsou přidány do důvěryhodné zóny síťového připojení, na které je tento profil aplikován (bez ohledu na typ ochrany sítě).

Důvěryhodné připojení - vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti (přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít při vytváření profilu pro zabezpečené připojení k místní síti. Všechny přímo připojené podsítě jsou rovněž považovány za důvěryhodné. Například, pokud je síťový adaptér připojen k síti s IP adresou 192.168.1.5 a maskou 255.255.255.0, podsíť 192.168.1.0/24 bude přidána do důvěryhodné zóny. Pokud má adaptér více adres/podsítí, budou důvěryhodné všechny.

Upozornit na slabě zabezpečenou Wi-Fi síť – po aktivování této možnosti ESET Endpoint Security zobrazí na ploše oznámení, jestliže se připojíte k nezabezpečené nebo slabě zabezpečené bezdrátové síti.

Spouštěče – vlastní podmínky, které musí být splněny, aby bylo možné přiřadit tento profil síťového připojení k určitému síťovému připojení. Podrobné vysvětlení naleznete v kapitole Spouštěče.

Spouštěče

Spouštěče jsou vlastní podmínky, které musí být splněny, aby bylo možné přiřadit Profil síťového připojení k Síťovému připojení. Pokud má připojená síť stejné atributy, jaké jsou definovány ve spouštěčích pro profil připojené sítě, bude profil na síť použit. Profil síťového připojení může mít jeden nebo více spouštěčů. Pokud existuje více spouštěčů, platí logika NEBO (musí být splněna alespoň jedna podmínka). Spouštěče můžete definovat v editoru profilu síťového připojení. Vytváření vlastních profilů síťového připojení by měl provádět zkušený uživatel.

K dispozici jsou následující Spouštěče (bližší informace o síti, ke které jste aktuálně připojeni, naleznete v kapitole Síťová připojení):

Adaptér

Typ adaptéru – profil se použije, pokud je síťové připojení navázáno pomocí vybraného typu adaptéru.
Název adaptéru – profil se použije, pokud odpovídá názvu síťového adaptéru.
IP adresa adaptéru – profil se použije, pokud odpovídá IP adrese síťového adaptéru.

DNS

Přípona DNS – profil se použije, pokud mu odpovídá název domény.
IP adresa DNS – profil se použije, pokud mu odpovídá IP adresa DNS serveru.

WINS

Profil se použije, pokud mu odpovídá IP adresa ve službě Windows Internet Name Service (WINS).

DHCP

DHCP IP – odpovídá IP adrese serveru DHCP.

Výchozí brána

IP – profil se použije, pokud mu odpovídá IP adrese výchozí brány.
MAC adresa – profil se použije, pokud se shoduje s MAC adresou výchozí brány.

Wi-Fi

SSID – profil se použije, pokud mu odpovídá SSID (název Wi-Fi).
Název profilu – profil se použije, pokud mu odpovídá název profilu Wi-Fi.
Typ zabezpečení – profil se použije, pokud typ zabezpečení odpovídá typu vybranému z rozbalovacího menu. (Pokud chcete, aby odpovídal více než jeden typ, vytvořte další spouštěč).
Typ šifrování – profil se použije, pokud typ šifrování odpovídá typu vybranému z rozbalovacího menu. (Pokud chcete, aby odpovídal více než jeden typ, vytvořte další spouštěč).
Zabezpečení sítě – profil se použije, pokud je síť **otevřená/zabezpečená**.

Profil systému Windows

Profil se použije, pokud je síť v systému Windows nakonfigurována jako **Doména/Privátní/Veřejná**.

Ověření

Autentifikace zóny vyhledává v síti specifický server a pro vlastní autentifikaci vůči serveru používá asymetrické šifrování (RSA). Název ověřované sítě musí odpovídat názvu v nastavení ověřovacího serveru. Mějte na paměti, že se v názvu rozlišuje velikost písmen. Název serveru lze zadat jako IP adresu, DNS nebo název NetBios.
Stáhnout ESET Authentication Server
Zdroj, ze kterého se bude načítán veřejný klíč, může být soubor typu:
• Veřejný klíč zašifrovaný ve formátu PEM (.pem); tento klíč můžete vygenerovat pomocí ověřovacího serveru ESET
• Šifrovaný veřejný klíč
• Certifikát s veřejným klíčem (.crt)
Pro ověření nastavení klikněte na tlačítko **Otestovat**. Pokud je ověření úspěšné, zobrazí se zpráva Autentifikace proběhla úspěšně. Pokud není ověřování správně nakonfigurováno, zobrazí se jedna z následujících chybových zpráv:
Autentifikace k serveru nebyla úspěšná. Neplatný nebo neodpovídající podpis.
Podpis serveru neodpovídá zadanému veřejnému klíči.
Autentifikace k serveru nebyla úspěšná. Název sítě neodpovídá.
Název zóny na klientovi se neshoduje s názvem zóny nastavené na autentifikačním serveru. Je nutné, aby zóny byly pojmenovány stejně.
Autentifikace k serveru nebyla úspěšná. Neplatná nebo žádná odpověď od serveru.
Žádná odpověď, server neběží nebo není dostupný. Neplatnou odpověď můžete obdržet, pokud na dané adrese běží jiný HTTP server.
Zadaný veřejný klíč je neplatný.
Ověřte, že je veřejný klíč zadán správně.

Sady IP adres

Sada IP adres je skupina IP adres, které vytvářejí jednu logickou skupinu adres IP, což je užitečné při opakovaném použití stejné sady adres ve více pravidlech firewallu nebo pravidlech ochrany proti útokům hrubou silou. ESET Endpoint Security obsahuje také předdefinované sady IP adres, pro které se použijí interní pravidla. Příkladem takové skupiny je **Důvěryhodná zóna**. Důvěryhodná zóna představuje skupinu síťových adres, ve které jsou váš počítač a v něm uložené sdílené soubory, viditelné pro ostatní uživatele sítě a ostatní uživatelé sítě mají přístup k systémovým prostředkům.

Přidání sady IP adres:

1. Otevřete Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Sady IP adres** > **Změnit.**
2. Klikněte na tlačítko **Přidat**, zadejte **název** a **popis** zóny, a nakonec zadejte **vzdálenou adresu počítače (definovanou pomocí IPv4/IPv6 adresy, rozsahu, masky)**.
3. Klikněte na tlačítko **OK**.

Další informace naleznete v kapitole Úprava sad IP adres.

Úprava sad IP adres

Další informace o sadách IP adres naleznete v kapitole Sady IP adres.

Sloupce

Název – název skupiny vzdálených počítačů.

Popis – obecný popis skupiny.

IP adresy – vzdálené IP adresy, které patří do sady IP adres.

Ovládací prvky

Při **přidávání** nebo **úpravách** sady IP adres jsou k dispozici následující pole:

Název – název skupiny vzdálených počítačů.

Popis – obecný popis skupiny.

Vzdálená adresa počítače (IPv4, IPv6, rozsah, podsíť) – umožní přidat vzdálenou adresu, rozsah adres nebo podsíť.

Odstranit – odebere zónu ze seznamu.

Předdefinované sady IP adres nelze odstranit.

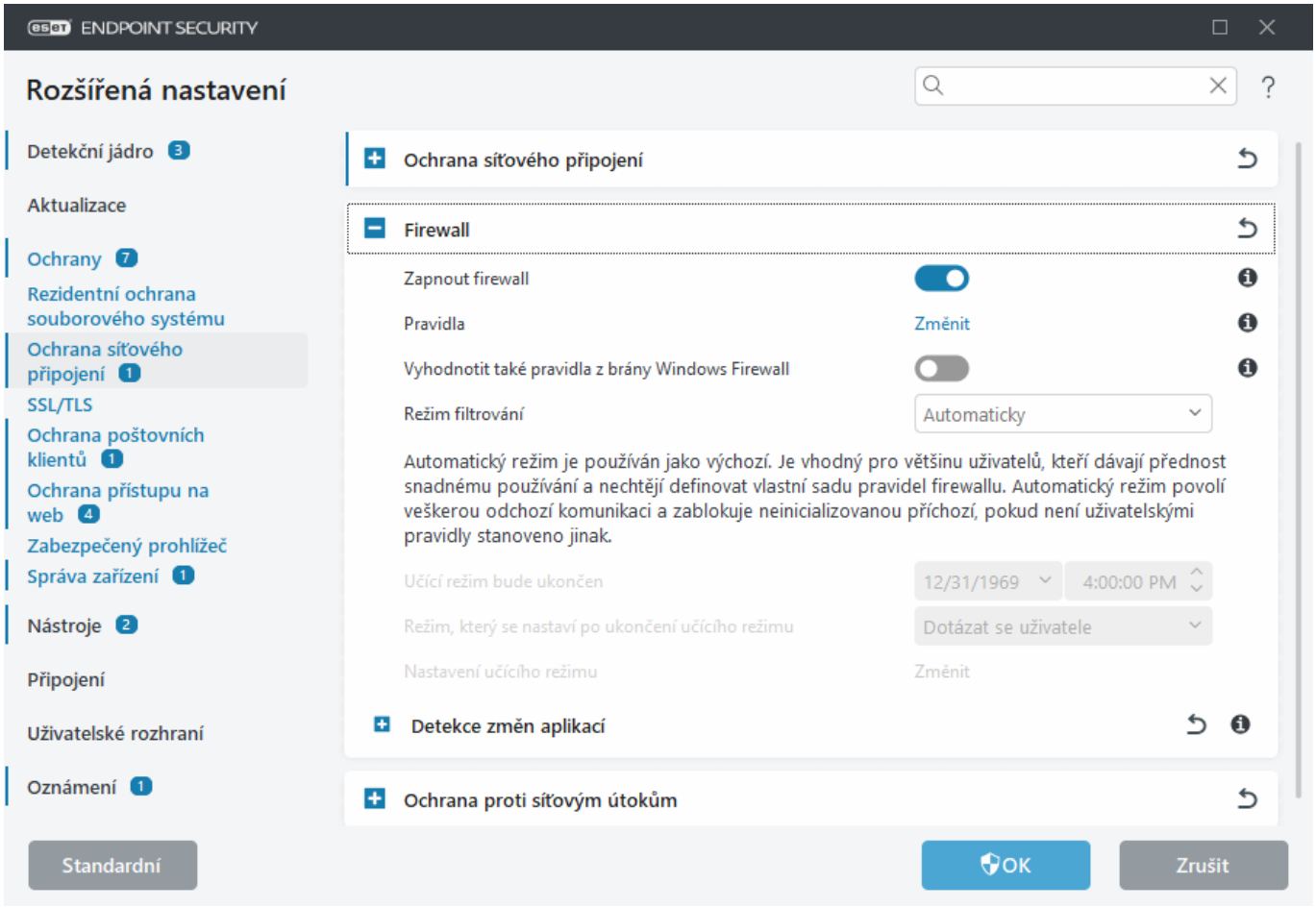
Příklady IP adres

Přidání IPv4 adresy:
Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).
Rozsah adres – umožní zadat počáteční a koncovou IP adresu pro rozsah IP několika zařízení (například *192.168.0.1-192.168.0.99*).
Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsíť 192.168.1.0. Chcete-li vyloučit celou podsíť, zadejte *192.168.1.0/24*.
Přidání IPv6 adresy:
Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podsíť – podsíť skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Firewall

Firewall řídí veškerý příchozí a odchozí síťovou komunikaci na vašem zařízení na základě interních a vámi definovaných pravidel. Toho se dosáhne povolením nebo zakázáním jednotlivých síťových připojení. Úkolem firewallu je zablokovat příchozí útoky ze vzdálených zařízení a blokovat nežádoucí služby a aplikace.

Chcete-li nakonfigurovat Firewall, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Firewall**.



Firewall

Zapnout firewall

Pro zajištění bezpečnosti systému doporučujeme ponechat tuto funkci aktivní. Pokud je Firewall povolen, síťová komunikace se kontroluje v obou směrech.

Pravidla

Nastavení pravidel umožňuje zobrazit a upravit všechna pravidla firewallu aplikovaná na komunikaci mezi aplikacemi v rámci důvěryhodných zón a internetu.

Nevyhodnocují se pravidla brány Windows Firewall definovaná zásadami skupiny (GPO).

V případě, že na váš počítač útočí Botnet, můžete si vytvořit pravidlo IDS. Pravidlo upravíte v části Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **IDS pravidla**, kliknutím na **Změnit**.

Vyhodnotit také pravidla z brány Windows Firewall

V režimu automatického filtrování také povolí příchozí provoz povolený pravidly z Windows Firewallu, pokud není výslovně blokován pravidly ESET.

Režim filtrování

Chování firewallu záleží na vybraném režimu. Zároveň ovlivňuje míru interakce s uživatelem.

Ve firewallu produktu ESET Endpoint Security jsou dostupné následující režimy pro filtrování komunikace:

Režim filtrování	Popis
Automatický režim	Přednastavený mód. Je určen pro uživatele, kteří preferují rychlé a pohodlné fungování firewallu bez nutnosti definování pravidel. Vlastní pravidla vytvářet můžete, ale nejsou pro běh **Automatického režimu** vyžadována. Tento režim povoluje veškerou komunikaci z daného systému směrem ven a blokuje většinu příchozí komunikace kromě komunikace z Důvěryhodné zóny (definované v IDS a rozšířeném nastavení/Povolené služby) odpovídající na nedávnou odchozí komunikaci na stejnou vzdálenou stranu.
Interaktivní režim	Umožňuje nastavení firewallu na míru podle požadavků uživatele. V případě zjištění jakékoli komunikace, na kterou není možné aplikovat žádné existující pravidlo, se uživateli zobrazí dialogové okno s výběrem akce. Následně je možné tuto komunikaci povolit nebo zamítnout, přičemž z tohoto rozhodnutí můžete vytvořit nové pravidlo. V takovém případě bude každá další komunikace tohoto typu v budoucnu povolena nebo zablokována, podle tohoto pravidla.
Administrátorský režim	– blokuje každé spojení, pro které neexistuje povolující pravidlo. Tento režim je určen pro pokročilé uživatele, kteří potřebují definovat pravidla pro konkrétní bezpečné spojení. Každá další nespecifikovaná komunikace je firewallem blokována.
Učící režim	Automaticky vytváří pravidla a je vhodný pro prvotní konfiguraci firewallu. Vytvoření pravidel proběhne bez interakce uživatele, protože ESET Endpoint Security pravidla vytvoří na základě předem definovaných parametrů. Tento režim není bezpečný a doporučujeme jej používat pouze krátkodobě po instalaci, dokud se nevytvoří pravidla pro veškerou nutnou komunikaci.

Učící režim bude ukončen – nastavte datum a čas, kdy se učící režim automaticky ukončí. Učící režim můžete také kdykoli ručně vypnout.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte, ke kterému režimu filtrování se vrátí firewall po ukončení učícího režimu. Další informace o režimech filtrování najdete v tabulce výše. Po dokončení vyžaduje možnost **Dotázat se uživatele** oprávnění administrátora k provedení změny režimu filtrování firewallu.

Nastavení učícího režimu – kliknutím na tlačítko **Upravit** nakonfigurujete parametry pro ukládání pravidel vytvořených v učícím režimu.

Detekce změn aplikací

Funkce Detekce změn aplikací zobrazí oznámení v případě, kdy se změněná aplikace, pro kterou existuje pravidlo brány firewall, pokusí navázat komunikaci.

Nastavení učícího režimu

Firewall produktu PRODUCTNAME obsahuje učící režim, ve kterém je pro každou komunikaci vytvořeno a uloženo odpovídající pravidlo. Vytváření pravidel probíhá bez interakce s uživatelem, protože jsou vytvářena na základě předdefinovaných parametrů.

Tento režim není bezpečný a doporučujeme jej používat pouze pro prvotní konfiguraci firewallu.

Chcete-li aktivovat možnosti Učícího režimu, vyberte možnost **Učení** z rozbalovacího menu vRozšířeném nastavení > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Režim filtrování**. Klikněte na **Upravit** vedle položky **Nastavení učícího režimu** a nakonfigurujte následující možnosti:

V učícím režimu firewall nefiltruje komunikaci. Povolená je veškerá odchozí a příchozí komunikace. Počítač v tomto režimu není plnohodnotně chráněn firewallem.

Příchozí komunikace z důvěryhodné zóny – vzdálený počítač z důvěryhodné zóny se pokouší komunikovat s lokální aplikací běžící na počítači.

Odchozí komunikace do důvěryhodné zóny – lokální aplikace se pokouší komunikovat s jiným počítačem v lokální síti nebo s jinou sítí v důvěryhodné zóně.

Příchozí komunikace z internetu – vzdálený počítač se pokouší komunikovat s aplikací běžící na počítači.

Odchozí komunikace do internetu – aplikace běžící na počítači se pokouší komunikovat se vzdáleným počítačem.

V každé sekci můžete definovat parametry nově vytvářených pravidel:

Přidat lokální port – číslo lokálního portu síťové komunikace. Pro odchozí spojení se generují náhodná čísla portů. Z tohoto důvodu doporučujeme tuto funkci povolit pouze pro příchozí komunikaci.

Přidat aplikaci – název lokální aplikace. Je doporučeno použít tehdy, pokud chcete do pravidla zahrnout kompletní komunikaci specifikované aplikace. Tedy např. povolit komunikaci pro prohlížeč webových stránek, poštovního klienta apod.

Přidat vzdálený port – číslo vzdáleného portu síťového spojení. Příkladem může být povolení nebo zakázání konkrétní služby se běžným číslem portu, např. HTTP – 80, POP3 – 110 apod.

Přidat vzdálenou IP adresu / důvěryhodnou zónu – vzdálená IP adresa nebo celá zóna adres může být použita jako parametr při vytváření nového pravidla, které se použije na všechny síťové spojení mezi lokálním systémem a těmito adresami. Vhodné použít v případě, pokud chcete definovat akce pro konkrétní zařízení nebo skupinu zařízení v síti.

Maximální počet různých pravidel pro jednu aplikaci – pokud aplikace komunikuje více směry (z různých portů, na různé IP adresy a pod.), poté pro ně firewall v učícím režimu vytvoří odpovídající počet pravidel. Tímto je možné omezit počet pravidel, které mohou být vytvořeny pro jednu aplikaci.

Dialogové okno – Ukončit učící režim

Po uběhnutí stanovené doby vyhrazené pro učící režim, budete vyzváni k přepnutí firewallu do **Interaktivního** nebo **Administrátorského** režimu filtrování. Ve chvíli, kdy běžel firewall v učícím režimu, byla vytvořena pravidla bez interakce uživatele.

Pro více informací o jednotlivých režimech filtrování přejděte do kapitoly Režimy filtrování.

Vytvořená pravidla v učícím režimu doporučujeme ručně zkontrolovat prostřednictvím **Editoru pravidel**.

Pravidla firewallu

Pravidla firewallu představují seznam podmínek, podle kterých jsou testována všechna síťová spojení, a jsou k nim přiřazené akce. V části Pravidla firewallu můžete definovat akce pro situace, kdy je navázáno několik síťových

spojení.

Pravidla jsou vyhodnocována shora dolů a jejich priorita je uvedena v prvním sloupci. Pro každou komunikaci se provede první vyhovující pravidlo.

Z hlediska směru komunikace je možné provést rozdělení spojení na příchozí a odchozí. Příchozí spojení je iniciováno na vzdálené straně a snaží se navázat spojení s lokální stranou. V případě odchozího spojení je situace opačná, tedy lokální strana navazuje spojení se vzdáleným počítačem.

V případě zjištění neznámé komunikace je potřeba zvážit, zda ji povolit nebo zamítnout. Nevyžádané, nezabezpečené nebo zcela neznámé spojení představuje pro systém bezpečnostní riziko. Při takové komunikaci je vhodné věnovat pozornost především vzdálené straně a aplikaci, která se pokouší navázat toto spojení. Mnoho infiltrací odesílá soukromá data nebo stahuje další škodlivé aplikace na počítač. Právě tato skrytá spojení je možné pomocí firewallu odhalit a zakázat.

Pravidla firewall můžete zobrazit a upravit v části Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Pravidla** > **Změnit**.

Pokud máte mnoho pravidel firewallu, můžete pomocí filtru zobrazit pouze konkrétní pravidla. Chcete-li filtrovat pravidla firewallu, klikněte na možnost **Další filtry** nad seznamem pravidel firewallu. Pravidla můžete filtrovat podle následujících kritérií:

- Původ
- Směr
- Akce
- Dostupnost

Ve výchozím nastavení jsou předdefinovaná pravidla firewallu skrytá. Chcete-li zobrazit všechna předdefinovaná pravidla, deaktivujte přepínač vedle položky **Skrýt vestavěná (předdefinovaná) pravidla**. Tato pravidla můžete deaktivovat, ale nemůžete je odstranit.

Klikněte na ikonu vyhledávání vpravo nahoře a vyhledejte pravidlo (pravidla).

Sloupce

Priorita – pravidla jsou vyhodnocována shora dolů a jejich priorita je uvedena v prvním sloupci.

Zapnuto - ukazuje, zda je pravidlo aktivní nebo ne; pro aktivaci pravidla musí být zaškrtnuto příslušné políčko.

Aplikace – název aplikace, pro kterou platí pravidlo.

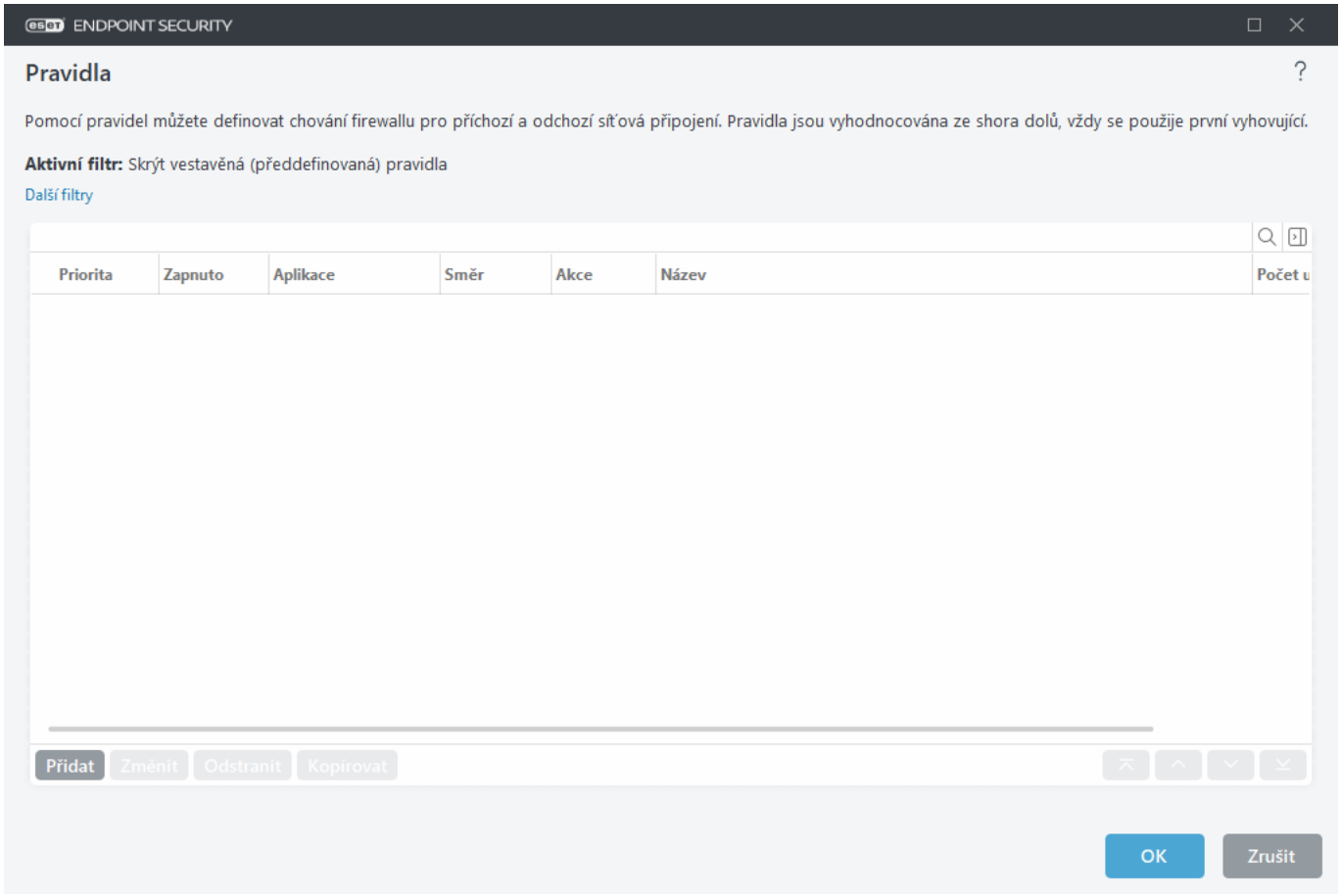
Směr – směr komunikace (příchozí/odchozí/oba).

Akce – akce, která se s komunikací provede (zablokovat/povolit/dotázat se).

Název – název pravidla. Ikona ESET představuje předdefinované pravidlo.

Počet uplatnění – celkový počet použití pravidla.

Kliknutím na ikonu rozbalení zobrazíte podrobnosti o pravidle.



Ovládací prvky

Přidat – kliknutím vytvoříte nové pravidlo.

Změnit – kliknutím upravíte existující pravidlo.

Odstranit – kliknutím odstraníte existující pravidlo.

Kopírovat – kliknutím vytvoříte kopii existujícího pravidla.

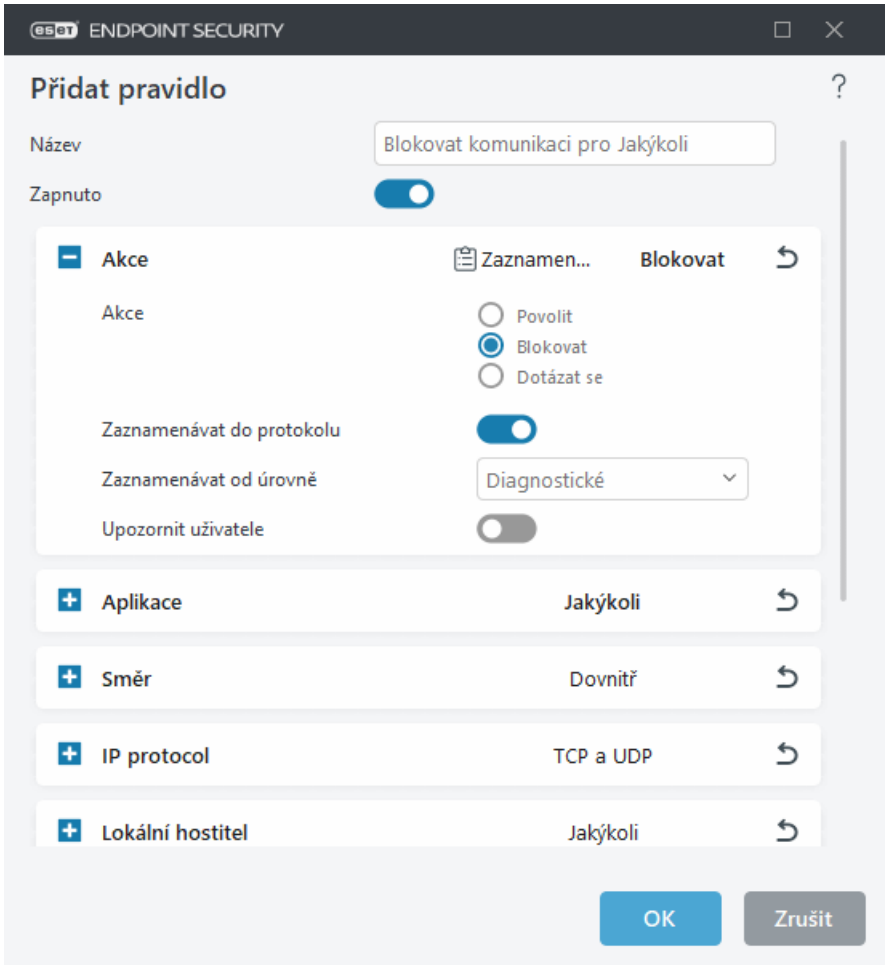
 **Nahoru/Výše/Dolů/Níže** – pomocí těchto tlačítek změníte pořadí vyhodnocování pravidel (vyhodnocována jsou shora dolů).

Přidání a úprava pravidel firewallu

Pravidla firewallu představují podmínky, podle kterých jsou testována všechna síťová připojení, a jsou k nim přiřazené akce. Vytvoření nového nebo změna stávajícího pravidla firewallu je vyžadována vždy, když dojde ke změně sledovaných parametrů spojení. V takovém případě totiž pravidlo již nesplňuje podmínku a není tedy na něj uplatněna definovaná akce. V konečném důsledku to může znamenat zamítnutí spojení a následné problémy s funkčností aplikace. Příkladem je změna síťové adresy vzdálené strany nebo čísla portu. Zkušený uživatel by měl vytvořit vlastní Pravidla firewallu.

Následující články z Databáze znalostí mohou být dostupné pouze v angličtině:
- Vytvoření nebo úprava pravidel firewallu v produktu ESET Endpoint Security
- Vytvoření nebo úprava pravidel firewallu pro klientské stanice v ESET PROTECT

Chcete-li přidat nebo upravit pravidlo firewallu, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Pravidla** > **Změnit**. V okně Pravidla firewallu klikněte na tlačítko **Přidat** nebo **Změnit**.



Název – zadejte název pravidla.

Povoleno – kliknutím na přepínač se pravidlo aktivuje.

Přidejte akce a podmínky pro pravidlo firewallu:

Akce

Akce – vyberte, zda chcete **Povolit** nebo **Blokovat** komunikaci, která odpovídá podmínkám definovaným v tomto pravidle, nebo zda se má ESET Endpoint Security **Dotázat** při každém navázání komunikace.
Zaznamenávat do protokolu - pokud bude pravidlo použito, bude zaznamenáno do Protokolů.
Zaznamenávat do úrovně – zvolte závažnost záznamu protokolu pro toto pravidlo.
Informovat uživatele zobrazí upozornění, pokud je pravidlo aplikováno.

Aplikace

Zadejte aplikaci, pro kterou bude toto pravidlo použito.
Cesta k aplikaci – klikněte na **...** a přejděte k aplikaci nebo zadejte celou cestu k ní (například C:\Program Files\Firefox\Firefox.exe). NEZADÁVEJTE pouze název aplikace.
Digitální podpis aplikace – pravidlo můžete použít na aplikace na základě jejich signatur (jména vystavitele). Z rozbalovacího menu vyberte, zda chcete pravidlo použít na aplikace s **Jakýmkoli platným podpisem** nebo na aplikace **Podepsané určitým vystavitelem**. Pokud vyberete aplikace **Podepsané určitým vystavitelem**, je třeba zadat vystavitele v poli **Jméno vystavitele**.
Aplikace z Microsoft Store – z rozbalovacího menu vyberte aplikaci nainstalovanou z Microsoft Store.
Služba – místo aplikace můžete vybrat systémovou službu. Otevřete rozbalovací menu a vyberte službu.
Použít na potomky procesu – některé aplikace mohou spouštět více procesů, zatímco vy vidíte pouze jedno okno aplikace. Povolením tohoto přepínače zajistíte, že se pravidlo bude vztahovat na každý proces pro zadanou aplikaci.

Směr

Vyberte **směr** komunikace, na který se bude toto pravidlo vztahovat:
- **Oba** – příchozí i odchozí komunikace
- **Dovnitř** – pouze příchozí komunikace
- **Ven** – pouze odchozí komunikace

IP protokol

Pokud chcete, aby se toto pravidlo vztahovalo pouze na určitý protokol, vyberte z rozbalovacího menu **Protokol**.

Lokální hostitel

Lokální adresy, rozsah adres nebo podsíť, pro které se toto pravidlo použije. Pokud není zadána žádná adresa, pravidlo se použije na veškerou komunikaci s lokálními hostiteli. IP adresy, rozsahy adres nebo podsítě můžete přidávat přímo do textového pole **IP adresa** nebo vybírat z existujících Sad IP adres kliknutím na tlačítko **Změnit** vedle položky **Sady IP adress**.

Lokální port

Číslo (čísla) lokálního **portu**. Pokud nejsou zadána žádná čísla potů, pravidlo se použije pro libovolný port. Můžete přidat jeden komunikační port nebo řadu komunikačních portů.

Vzdálený hostitel

Vzdálená adresa, rozsah adres nebo podsíť, pro kterou se toto pravidlo použije. Pokud není zadána žádná adresa, pravidlo se použije na veškerou komunikaci se vzdálenými hostiteli. IP adresy, rozsahy adres nebo podsítě můžete přidávat přímo do textového pole **IP adresa** nebo vybírat z existujících Sad IP adres kliknutím na tlačítko **Změnit** vedle položky **Sady IP adress**.

Vzdálený port

Číslo(a) vzdáleného **portu**. Pokud nejsou zadána žádná čísla potů, pravidlo se použije pro libovolný port. Můžete přidat jeden komunikační port nebo řadu komunikačních portů.

Profil

Pravidlo firewallu lze použít na konkrétní profily síťových připojení.
Jakýkoli – pravidlo bude použito na jakékoli síťové připojení bez ohledu na použitý profil.
Vybráno – pravidlo bude použito na konkrétní síťové připojení na základě vybraného profilu. Zaškrtněte políčko vedle profilů, které chcete vybrat.

Vytvoříme nové pravidlo, které povolí webovému prohlížeči Firefox přistupovat k internetu / lokálním webovým stránkám.
1. V sekci **Akce** vyberte možnost **Akce** > **Povolit**.
2. V sekci **Aplikace** zadejte **Cestu k aplikaci** webového prohlížeče (např. C:\Program Files\Firefox\Firefox.exe). NEZADÁVEJTE pouze název aplikace.
3. V sekci **Směr** vyberte možnost **Směr** > **Ven**.
4. V sekci **IP protokol** vyberte z rozbalovacího menu **Protokol TCP a UDP**.
5. V sekci **Vzdálený port** přidejte čísla **portů**: *80,443* pro standardní internetové procházení.

Mějte na paměti, že předefinovaná pravidla není možné měnit, pouze je můžete deaktivovat.

Detekce změn aplikací

Funkce detekce změn aplikací zobrazí upozornění v případě, kdy se změněná aplikace, pro kterou existuje pravidlo brány firewall, pokusí navázat komunikaci. Změna aplikace je mechanismus dočasného nebo trvalého nahrazení původní aplikace novou aplikací za pomoci jiného spustitelného souboru (chrání před zneužitím pravidel brány firewall).

Tato funkce není určena pro detekci změn všech aplikací. Cílem této funkce je zabránit zneužití existujících pravidel firewallu, proto jsou monitorovány pouze aplikace, pro které existují pravidla.

Chcete-li upravit **Detekce změn aplikací**, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Detekce změn aplikací**.

Kontrolovat změnu aplikací – pokud je tato možnost aktivní, program bude sledovat, zda se daná aplikace změnila (aktualizovala, infikovala, jinak změnila). Hlášení o změně aplikace se zobrazí ve chvíli, kdy aplikace navazuje komunikaci.

Povolit změnu podepsaných (důvěryhodných) aplikací – o změně aplikací, které jsou digitálně podepsány nebudete informováni.

Seznam aplikací vyloučených z detekce – umožňuje přidat nebo odebrat aplikace, u kterých jsou povoleny změny bez oznámení.

Seznam aplikací vyloučených z detekce

Firewall produktu ESET Endpoint Security detekuje změny aplikací, pro které existuje pravidlo. Pro více informací přejděte do kapitoly Detekce změn aplikací.

Pokud nechcete, aby konkrétní aplikace, pro kterou existuje pravidlo ve firewallu, byla sledována, můžete ji z monitorování vyloučit.

Přidat – po kliknutí se zobrazí dialogové okno, ve kterém můžete definovat aplikaci, kterou chcete vyloučit z detekce změn. Aplikaci můžete vybrat z již existujícího seznamu, které běží v systému a existuje pro ně pravidlo ve firewallu, případně zadejte cestu k aplikaci ručně.

Změnit – po kliknutí se zobrazí dialogové okno, ve kterém můžete upravit existující výjimku pro aplikaci vyloučenou z detekce změn. Jinou aplikaci si můžete vybrat z již existujícího seznamu, které běží v systému a existuje pro ně pravidlo ve firewallu, případně zadejte cestu k aplikaci ručně.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu aplikací vyloučených z detekce změn.

Ochrana proti síťovým útokům (IDS)

Ochrana proti síťovým útokům (IDS) zlepšuje detekci zneužití známých zranitelností. Více informací o tomto typu ochrany se můžete dočíst ve slovníku pojmů. Chcete-li nakonfigurovat ochranu proti síťovým útokům, otevřete Rozšířená nastavení > **Ochrana** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům**.

Zapnout ochranu proti síťovým útokům (IDS) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Komunikace, která bude vyhodnocena jako škodlivá, bude blokována.

Zapnout ochranu proti zapojení do botnetu – funkce dokáže na základě typických vzorů detekovat a zablokovat komunikaci mezi škodlivým kódem ve vašem počítači a řídícími (C&C) servery botnetu. Více informací o této ochraně se můžete dočíst ve slovníku pojmů.

IDS pravidla – umožňují nastavit pokročilé možnosti filtrování pro detekci několika typů útoků a zneužití, které by mohly poškodit váš počítač.

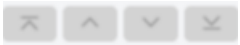
Všechny důležité události zaznamenané síťovou ochranou jsou ukládané do protokolů. Další informace naleznete v kapitole Protokol síťové ochrany.

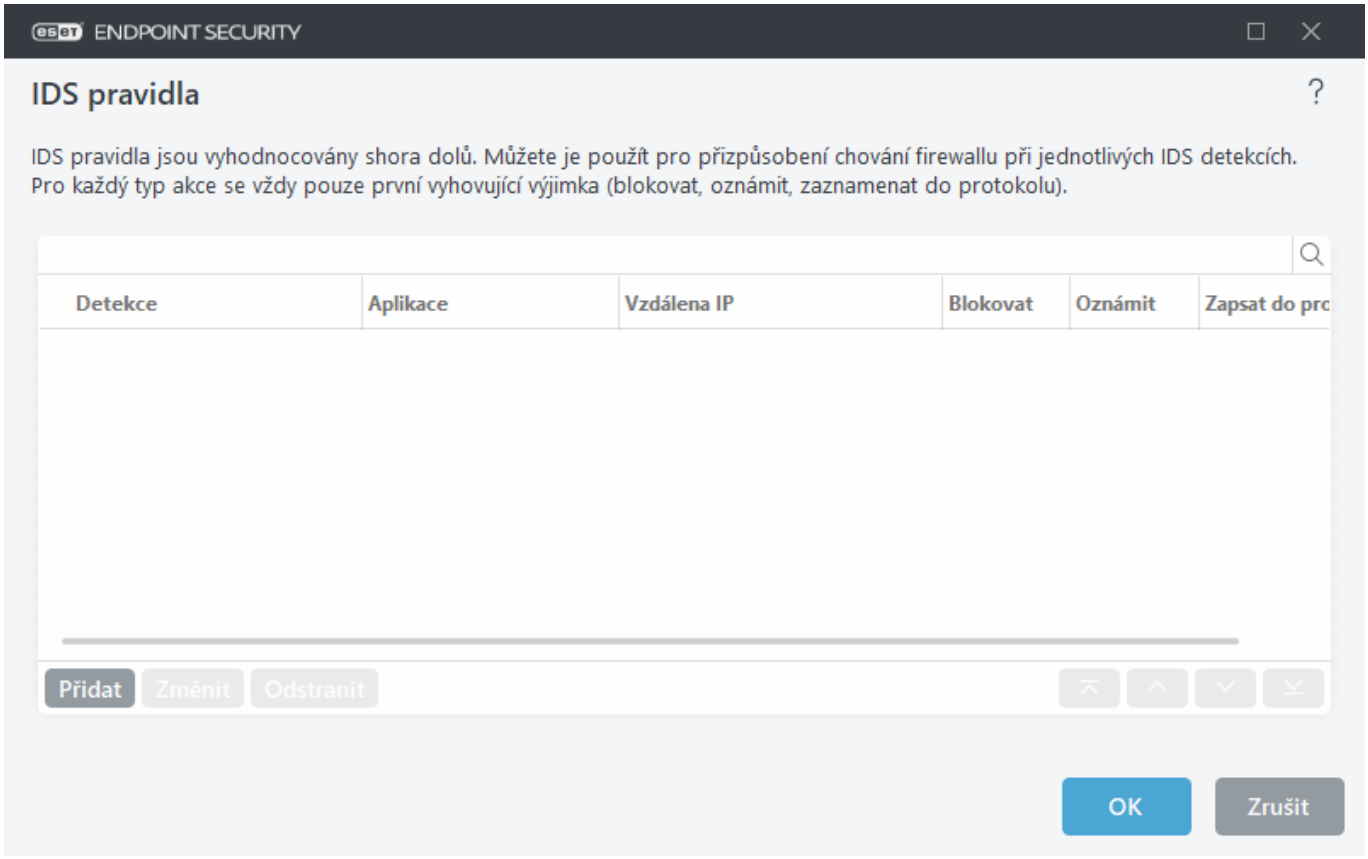
IDS pravidla

V některých případech může Intrusion Detection Service (IDS) detekovat komunikaci mezi routery nebo jinými interními síťovými zařízeními jako možný útok. Pokud je vám známá bezpečná adresa blokována, přidejte ji do Adres vyloučených z ochrany IDS pro obejití IDS.

Následující články z Databáze znalostí mohou být dostupné pouze v angličtině:
- Vytvoření IDS pravidla pro klientskou stanici v produktu ESET Endpoint Security
- Vytvoření IDS pravidla pro klientskou stanici prostřednictvím ESET PROTECT

Správa IDS pravidel

- **Přidat** – kliknutím vytvoříte nové IDS pravidlo.
- **Změnit** – kliknutím upravíte existující IDS pravidlo.
- **Odstranit** – vyberte IDS pravidlo, které chcete odstranit a klikněte na toto tlačítko.
-  **Šipky Nahoru/Výše/Dolů/Níže** – pomocí těchto tlačítek změníte pořadí vyhodnocování pravidel (výjimky jsou vyhodnocovány shora dolů).



Záložka **Výjimky** se zobrazí v případě, že administrátor vytvoří IDS výjimky ve webové konzoli ESET PROTECT. Na seznamu IDS výjimek se mohou nacházet pouze povolovací pravidla. Vyhodnocována jsou dříve, než IDS pravidla.

Editor pravidel

Detekce – typ detekce.

Název hrozby – pro některé dostupné detekce můžete zadat název hrozby.

Aplikace – kliknutím na … vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace.

Vzdálená IP adresa – seznam IPv4 nebo IPv6 adres / rozsahů adres / podsítí. Více záznamů oddělte čárkou.

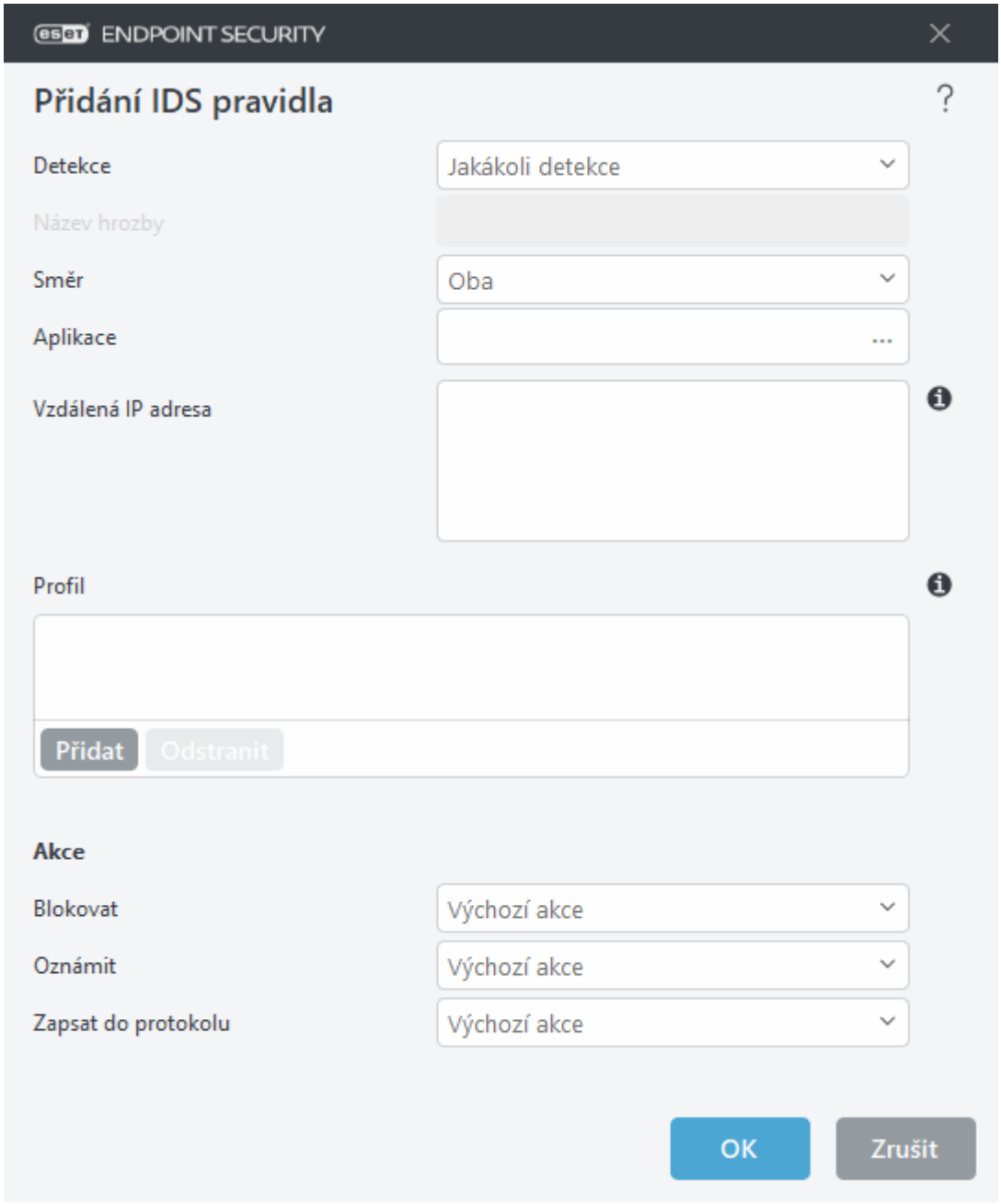
Profil – můžete vybrat profil síťového připojení, na který se toto pravidlo bude vztahovat.

Akce

Blokovat – nad každým systémovým procesem bude provedena standardní akce (povolit nebo blokovat). Pro změnu výchozího chování produktu ESET Endpoint Security vyberte z rozbalovacího menu požadovanou akci.

Oznámit – možnost Ano vyberte pro zobrazení Oznámení na pracovní ploše vašeho počítače. Možnost Ne vyberte, pokud nechcete oznámení na ploše zobrazovat. Dostupné možnosti: Výchozí akce/Ano/Ne.

Zapsat do protokolu – možnost **Ano** vyberte pro zapsání události do protokolu produktu ESET Endpoint Security. Možnost **Ne** vyberte, pokud nechcete událost zaznamenat do protokolu. Dostupné možnosti: **Výchozí akce**/**Ano**/**Ne**.



Pro zobrazení oznámení při výskytu každé události a jejího zaznamenání do protokolu:
1. Klikněte na tlačítko **Přidat** pro vytvoření nového IDS pravidla.
2. Z rozbalovací nabídky **Detekce** vyberte konkrétní upozornění.
3. Klikněte na **…** a vyberte cestu k aplikaci, na kterou chcete dané oznámení aplikovat.
4. V rozbalovacím menu **Blokovat** ponechte možnost **Výchozí akce**. Tím se provede výchozí akce produktu ESET Endpoint Security.
5. V rozbalovacím menu **Oznámit** a **Zapsat do protokolu** vyberte možnost **Ano**.
6. Oznámení uložte kliknutím na tlačítko **OK**.

Pro zrušení zobrazování oznámení pro konkrétní detekci, kterou nepovažujete za hrozbu:
1. Klikněte na tlačítko **Přidat** pro vytvoření nové IDS výjimky.
2. Z rozbalovacího menu **Detekce** vyberte vámi požadovanou upozornění, například **SMB relace bez bezpečnostního rozšíření** nebo **TCP Port Scanning attack**.
3. Jedná-li se o příchozí komunikaci, jako směr vyberte v rozbalovacím menu možnost **Dovnitř**.
4. V rozbalovacím menu **Oznámit** vyberte možnost **Ne**.
5. V rozbalovacím menu **Zapsat do protokolu** vyberte možnost **Ano**.
6. Pole **Aplikace** ponechte prázdné.
7. Pokud komunikace nepřichází pouze z konkrétní IP adresy, ponechte prázdné pole **Vzdálena IP adresa**.
8. Oznámení uložte kliknutím na tlačítko **OK**.

Ochrana proti útokům hrubou silou

Ochrana proti útokům hrubou silou blokuje pokusy o uhádnutí hesel pro RDP a SMB služby. Útok hrubou silou je metoda, kdy se systematicky zkouší možné kombinace písmen, číslic a znaků za účelem prolomení hesla. Chcete-li nakonfigurovat Ochranu proti útokům hrubou silou, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Ochrana proti útokům hrubou silou**.

Zapnout ochranu proti útoku hrubou silou – tato součást produktu ESET Endpoint Security sleduje obsah síťové komunikace a dokáže blokovat pokusy o uhádnutí hesel.

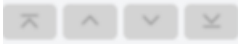
Pravidla – v editoru pravidel ochrany proti útokům hrubou silou si můžete zobrazit existující pravidla pro příchozí a odchozí síťová spojení, stejně tak si vytvářet vlastní a kdykoli je upravovat. Další informace naleznete v kapitole Pravidla.

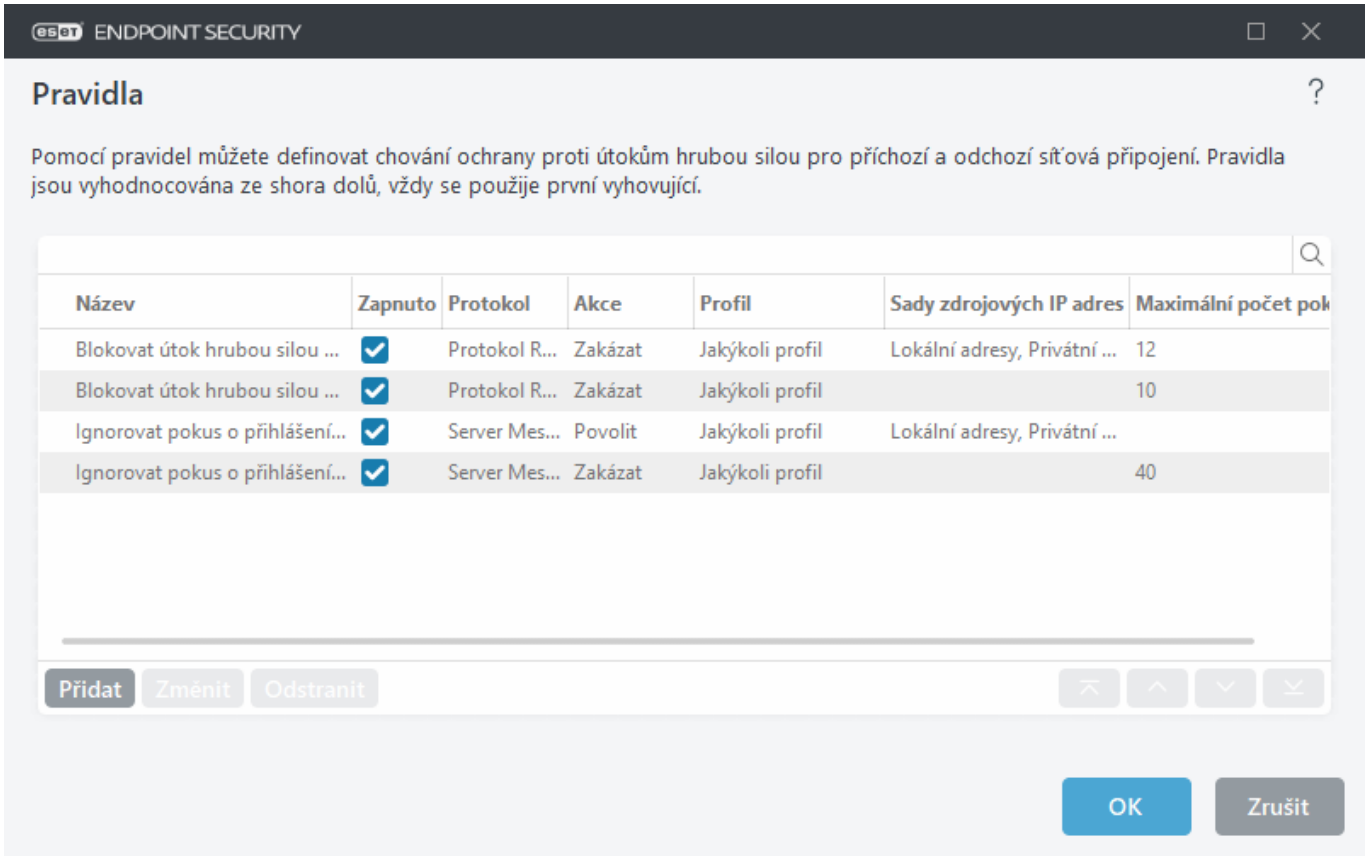
Výjimky – seznam detekcí vyloučených z kontroly definovaný na základě IP adresy nebo cesty k aplikaci. Výjimky je možné vytvářet a upravovat v konzoli ESET PROTECT. Další informace naleznete v kapitole Výjimky.

Pravidla

V editoru pravidel ochrany proti útokům hrubou silou si můžete zobrazit existující pravidla pro příchozí a odchozí síťová spojení, stejně tak si vytvářet vlastní a kdykoli je upravovat. Předdefinovaná pravidla není možné upravit ani odstranit.

Správa pravidel ochrany proti útokům hrubou silou

- **Přidat** – kliknutím vytvoříte nové pravidlo ochrany proti útokům hrubou silou.
- **Změnit** – kliknutím upravíte existující pravidlo ochrany proti útokům hrubou silou.
- **Odstranit** – vyberte IDS pravidlo, které chcete odstranit a klikněte na toto tlačítko.
-  Nahoru/Výše/Dolů/Níže – umožní přizpůsobit pořadí vyhodnocování pravidel (vyhodnocovány jsou ze shora dolů).



Pro zajištění nejvyšší míry ochrany se pravidlo s nejnižším **maximálním počtem pokusů** uplatní i v případě, kdy se v seznamu nachází níže, než ostatní pravidla vyhovující podmínkám detekce.

Editor pravidel

Název – název pravidla.

Zapnuto – deaktivujte tuto možnost pomocí přepínače, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Akce – rozhodněte se, zda chcete při splnění pravidlem definovaných podmínek spojení **zamítnout** nebo **povolit**.

Protokol – informace, pro který síťový protokol pravidlo platí.

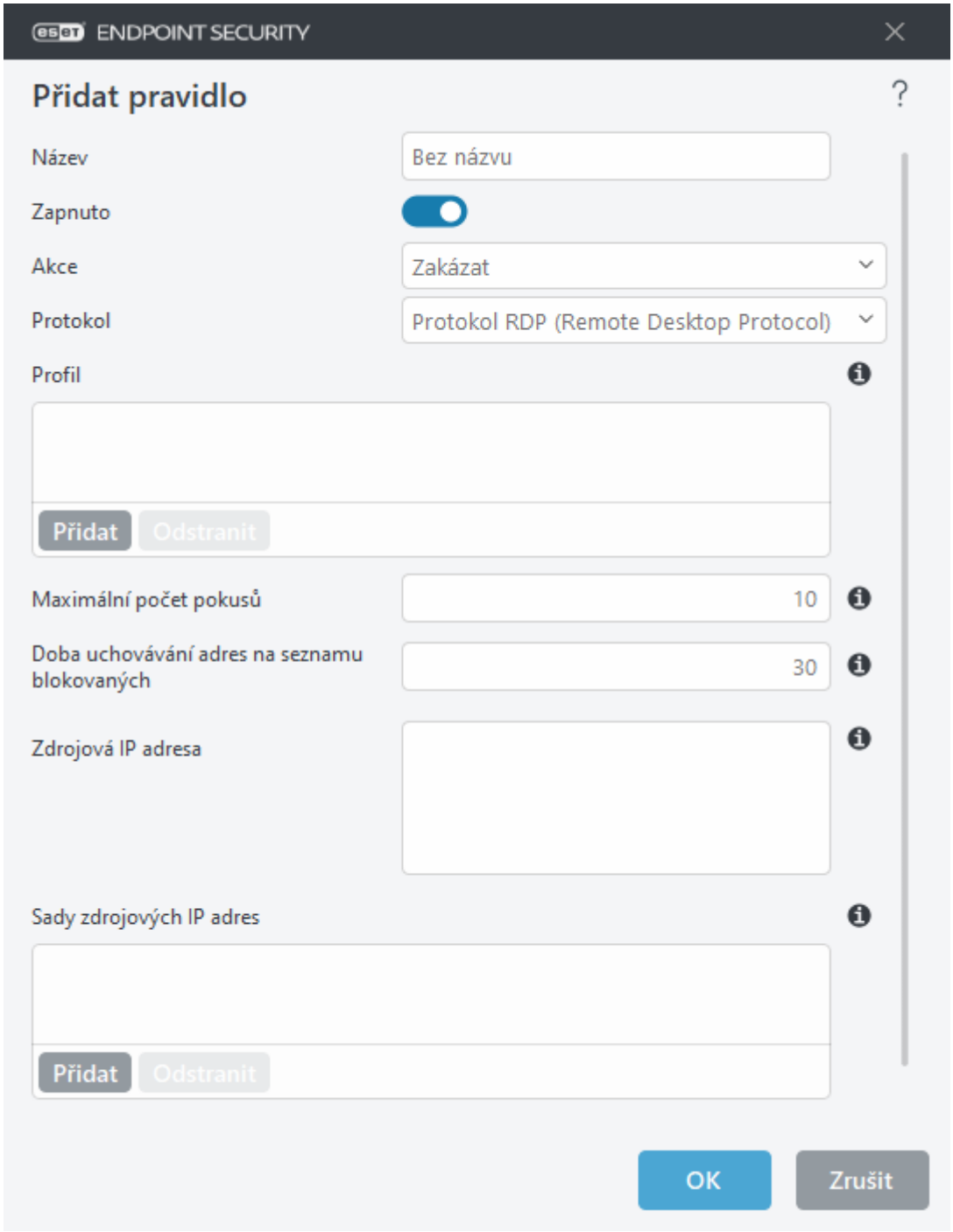
Profil – můžete vybrat profil síťového připojení, na který se toto pravidlo bude vztahovat.

Maximální počet pokusů – maximální počet povolených pokusů o opakování útoku, dokud nebude IP adresa zablokována a přidána na seznam blokovaných.

Doba uchovávání adres na seznamu blokovaných – definujte dobu, za jak dlouho bude adresa odstraněna ze seznamu blokovaných.

Zdrojová IP adresa – seznam IP adres, rozsahů nebo podsítí. Více záznamů oddělte čárkou.

Sady zdrojových IP adres – sada IP adres, které jste již definovali v Sadách IP adres.



Výjimky

Prostřednictvím výjimek na útoky hrubou silou můžete na základě specifického kritéria potlačit detekci útoku hrubou silou. Tyto výjimky je možné vytvořit v ESET PROTECT na základě detekce útoku hrubou silou.

Sloupce

- **Detekce** – typ detekce.
- **Aplikace** – kliknutím na … vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace.
- **Vzdálená IP** – seznam IPv4, IPv6 adres / rozsahů adres / podsítí. Více záznamů oddělte čárkou.

Správa výjimek

Seznam výjimek se zobrazí v případě, kdy administrátor vytvoří výjimku v ESET PROTECT Web Console. Na seznamu výjimek se mohou nacházet pouze povolovací pravidla. Vyhodnocována jsou dříve, než IDS pravidla.

Rozšířená nastavení

V části Rozšířená nastavení > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Další možnosti** můžete povolit nebo zakázat detekci několika typů útoků a exploitů, které mohou poškodit váš počítač.

V některých případech neobdržíte oznámení o hrozbě týkající se blokované komunikace. Informace o tom, jak zobrazit veškerou zablokovanou komunikaci firewallem naleznete v kapitole Protokolování a vytváření pravidel nebo výjimek z protokolu.

Dostupnost jednotlivých možností závisí na typu a verzi produktu ESET, zda je vybaven firewallem, a stejně tak na verzi operačního systému.

Detekce útoků

- **Protokol SMB**– k dispozici jsou možnosti pro blokování mnoha zranitelností v SMB protokolu:
- **Detekce útoku škodlivého serveru challenge autentifikací** – tato možnost chrání před útoky, které zneužívají autentifikaci pro získání uživatelských údajů.
- **Detekce úniku IDS během otevírání pojmenované roury** – detekce známých technik používaných pro navázání MSRPCS pojmenovaných rour v SMB protokolu.
- **Detekce CVE** (Common Vulnerabilities and Exposures) – detekce známých útoků, zranitelností a bezpečnostních děr pro zabránění útoku pomocí SMB protokolu. Pro více informací přejděte na webové stránky CVE na cve.mitre.org.
- **Protokol RPC** – detekce a blokování CVE v systémové službě vzdálené volání procedur určené pro Distributed Computing Environment (DCE).
- **Protocol RDP** – detekce a blokování CVE v RDP protokolu (viz výše).
- **Detekce útoku ARP Poisoning** – zabraňuje tzv. man-in-the-middle útokům a odhaluje odposlouchávání paketů síťových switchů, tedy stav, kdy útočník předává ostatním zařízením v síti falešné informace. ARP (Address Resolution Protocol) se používá při získávání a přiřazování IP adres zařízením v síti.
- **Detekce útoku skenování TCP/UDP portů** – zabraňuje útokům software, který se pokouší zjistit otevřené porty v počítači, které lze zneužít k napadení počítače. Více o tomto typu útoku se můžete dočíst ve slovníku pojmů.
- **Blokovat nebezpečnou adresu po detekci útoku** – IP adresy detekované jako zdroje útoků jsou přidány do seznamu blokovaných adres, aby se po určitou dobu zabránilo připojení. Můžete nastavit **Dobu uchovávání adres na seznamu blokovaných**, která nastavuje dobu, po kterou bude adresa po detekci útoku blokována.
- **Upozornit na detekci útoků** – po detekci útoku se zobrazí upozornění v pravém dolním rohu obrazovky v oznamovací oblasti.
- **Upozornit na příchozí útoky využívající bezpečnostní zranitelnosti** – k upozornění dojde, pokud bude zjištěn pokus o zneužití bezpečností díry, případně bude zaznamenán pokus o zneužití zranitelnosti k přístupu do systému.

Kontrola paketů

- **Povolit příchozí spojení k správcovským sdíleným položkám prostřednictvím SMB protokol** – administrativní sdílení jsou standardní síťová sdílení, které sdílí celé diskové oddíly (*C$*, *D$*, …) stejně jako systémové složky (*ADMIN$)*. Zakázáním připojení k administrátorským sdíleným položkám snížíte bezpečnostní riziko. Například červ Conficker provádí slovníkový útok pro získání přístupu k administrátorským sdíleným položkám.

- **Zakázat staré (nepodporované) SMB dialekty** – zakáže SMB relaci se starým dialektem SMB, který nepodporuje IDS. Nejnovější operační systémy Windows podporují staré dialekty SMB z důvodu zpětné kompatibility s předchozími verzemi, například Windows 95. Útočník může využít starší dialekt SMB záměrně, aby se vyhnul kontrole paketů. Zakažte staré SMB dialekty, pokud nepotřebujete sdílet soubory se staršími verzemi operačního systému Windows.
- **Zakázat zabezpečení SMB bez bezpečnostních rozšíření** – bezpečnostní rozšíření mohou být využita během navazování SMB relace pro zajištění bezpečnostní autentifikace pomocí mechanismu LAN Manager Challenge/Response (LM). Schéma LM je považované za slabé a nedoporučuje se jej používat.
- **Zakázat otevření spustitelného souboru na serveru mimo Důvěryhodnou zónu pomocí SMB protokolu** – zabraňuje komunikaci v případě, že se snažíte otevřít spustitelný soubor (.exe, .dll) ze sdílené složky na serveru, který nepatří do důvěryhodné zóny v firewallu. Kopírování spustitelných souborů ze zdrojů v důvěryhodné zóně je legitimní. Tato funkce by měla minimalizovat nebezpečí otevření nežádoucího souboru na škodlivém serveru, například když omylem kliknete na odkaz vedoucí na spustitelný soubor umístěný na škodlivém serveru.
- **Zakázat NTLM autentifikaci pomocí SMB protokolu při připojení na server v/mimo Důvěryhodnou zónu** – protokoly využívající autentifikační schéma NTLM (obě verze) jsou ohrožené útoky přeposílající přihlašovací údaje (známé jako SMB relay). Zakázáním autentifikace NTLM se servery mimo důvěryhodnou zónu omezíte nebezpečí přeposílání přihlašovacích údajů škodlivým serverem mimo důvěryhodnou zónu. Můžete také zakázat NTLM autentifikaci se servery v Důvěryhodné zóně.

- **Povolit komunikaci se službou Security Account Manager** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SAMR].

- **Povolit komunikaci se službou Local Security Authority** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-LSAD] a [MS-LSAT].

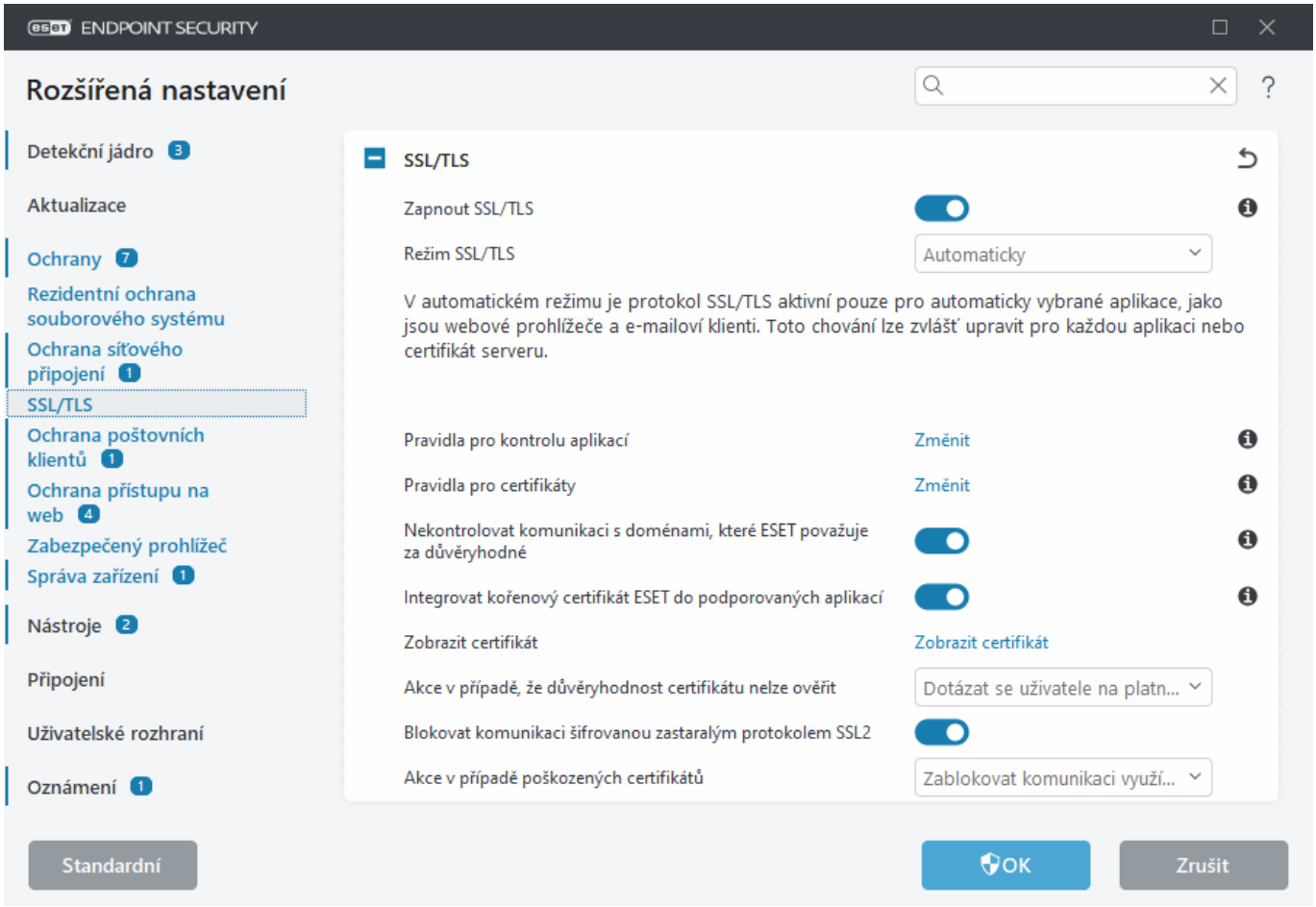
- **Povolit komunikaci se službou Vzdálený registr** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-RRP].

- **Povolit komunikaci se službou Správce řízení služeb** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SCMR].

- **Povolit komunikaci se službou Server** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SRVS].
- **Povolit komunikaci s ostatními službami** – ostatní MSRPC služby. MSRPC je implementace DCE RPC mechanismu ve Windows. Kromě toho MSRPC může používat pojmenované roury pro SMB (síťové sdílení souborů) protokol. Služba MSRPC (Microsoft RPC) poskytuje přístup k rozhraní pro vzdálený přístup a ovládání systému Windows. V systému MSRPC bylo objeveno několik zranitelností, které zneužil například červ Conficker, červ Sasser, aj. Zakázáním komunikace s MSRPC službami, které nepotřebujete, minimalizuje bezpečnostní riziko (jako například vzdálené spouštění kódu po sítí nebo pád služeb kvůli útoku).

SSL/TLS

ESET Endpoint Security může kontrolovat komunikační hrozby, které používají SSL protokol. Filtrování můžete přizpůsobit podle toho, zda je certifikát využívaný danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL. Chcete-li upravit nastavení SSL/TLS, otevřete Rozšířená nastavení > **Ochrany** > **SSL/TLS**.



Zapněte SSL/TLS – jestliže je vypnuto, ESET Endpoint Security nebude kontrolovat komunikaci přes SSL/TLS.

K dispozici jsou následující **režimy SSL/TLS**:

Režim filtrování	Popis
Automaticky	Výchozí režim, ve kterém je kontrolována pouze komunikace vybraných aplikací, jako jsou webové prohlížeče a poštovní klienti. Můžete jej přepsat výběrem aplikací, u kterých se komunikace kontroluje.
Interaktivní	Při přístupu k nové stránce zabezpečené protokolem SSL (s neznámým certifikátem) se zobrazí dialogové okno s výběrem akce. V tomto režimu můžete vytvořit seznam SSL certifikátů / aplikací, které chcete vyloučit z kontroly.
Administrátorský režim	Tuto možnost vyberte, pokud chcete kontrolovat veškerou komunikaci zabezpečenou protokolem SSL kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru s nedůvěryhodným certifikátem označeným jako důvěryhodný (je v seznamu důvěryhodných certifikátů) je komunikace se serverem povolena a obsah komunikačního kanálu je filtrován.

Pravidla pro kontrolu aplikací – umožňují přizpůsobit chování ESET Endpoint Security pro konkrétní aplikace.

Pravidla pro certifikáty – umožňují přizpůsobit chování ESET Endpoint Security pro konkrétní SSL certifikáty.

Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné – pokud je tato volba povolena, bude komunikace s důvěryhodnými doménami vyloučena z kontroly. Vestavěný seznam povolených adres spravovaný společností ESET určuje důvěryhodnost domény.

Integrovat kořenový certifikát ESET do podporovaných aplikací – aby SSL komunikace správně fungovala ve vašich prohlížečích a e-mailových klientech, je nezbytné, aby byl kořenový certifikát společnosti ESET přidán do seznamu známých kořenových certifikátů (vydavatelů). Pokud je tato možnost zapnutá, ESET Endpoint Security automaticky přidá certifikát ESET SSL Filter CA do známých prohlížečů ve vašem počítači (např. do prohlížeče Opera). Do prohlížečů využívajících systémové úložiště kořenových certifikátů se certifikát přidá automaticky. Např. Firefox je automaticky nastaven tak, aby důvěřoval kořenovým autoritám nacházejícím se v systémovém úložišti certifikátů.

V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát** > **Detaily** > **Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

Akce v případě, že důvěryhodnost certifikátu nelze ověřit – v některých případech nelze certifikát webové stránky ověřit pomocí TRCA (Trusted Root Certification Authorities), například vypršela platnost certifikátu, certifikát není důvěryhodný, certifikát není platný pro danou doménu nebo podpis, který lze zpracovat, ale nepodepisuje správně. Legitimní webové stránky vždy používají důvěryhodné certifikáty. Pokud je neposkytují, může to znamenat, že útočník dešifruje vaši komunikaci nebo že webové stránky mají technické potíže.

Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (ve výchozím nastavení je vybrána), při navázání šifrované komunikace se zobrazí okno s výběrem akce. V zobrazeném dialogovém okně pro výběr akce můžete certifikát označit jako důvěryhodný nebo vyloučený. Pokud se certifikát nenachází v TRCA, okno bude červené. V opačném případě bude okno zelené.

Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** vždy zablokujete komunikaci s webovou stránkou využívající nedůvěryhodný certifikát.

Blokovat komunikaci šifrovanou zastaralým protokolem SSL2 – komunikace pomocí starší verze protokolu SSL protokolu bude automaticky blokována.

Akce v případě poškozených certifikátů – poškozený certifikát znamená, že certifikát používá formát, který ESET Endpoint Security nerozpoznává, nebo byl přijat poškozený (například přepsaný náhodnými daty). V tomto případě doporučujeme ponechat zvolenou možnost **Zakázat komunikaci využívající daný certifikát**. Pokud vyberete **Dotázat se uživatele na platnost certifikátů**, uživatel bude vyzván k výběru akce po navázání šifrované komunikace.

Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
- Upozornění na certifikát v produktu ESET
- Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"

Pravidla pro kontrolu aplikací

Pomocí **Pravidel pro kontrolu aplikací** můžete přizpůsobit chování ESET Endpoint Security u konkrétních aplikací a zapamatovat si vybrané akce, pokud je **Režim filtrování protokolu SSL/TLS** nastaven v **Interaktivním režimu**.

Seznam lze zobrazit a upravit v části Rozšířená nastavení > **Ochrany** > **SSL/TLS** > **Pravidla pro kontrolu aplikací** > **Změnit**.

Okno **Pravidla pro kontrolu aplikací** se skládá z:

Sloupce

Aplikace – vyberte spustitelný soubor kliknutím na **…** nebo zadejte cestu k souboru ručně.

Akce při kontrole – pro kontrolu nebo ignorování komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – kliknutím přidáte filtrovanou aplikaci.

Změnit – vyberte aplikaci, kterou chcete konfigurovat a klikněte na tlačítko **Změnit**.

Odstranit – vyberte aplikaci, kterou chcete odstranit a klikněte na tlačítko **Odstranit**.

Importovat/Exportovat – seznam aplikací můžete importovat ze souboru, případně si jej a uložit pro budoucí použití.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

Pravidla pro certifikáty

Pravidla pro certifikáty lze použít k přizpůsobení chování ESET Endpoint Security pro konkrétní certifikáty SSL a k zapamatování akcí zvolených v **režimu SSL/TLS** v **interaktivním režimu**. Seznam lze zobrazit a upravit v části Rozšířená nastavení > **Ochrany** > **SSL/TLS** > **Pravidla pro certifikáty** > **Změnit**.

Okno **Pravidla pro certifikáty** se skládá z:

Sloupce

Název – název certifikátu.

Vydavatel certifikátu – jméno autora certifikátu.

Předmět certifikátu – identifikace entity asociované s veřejným klíčem uloženým v poli předmět veřejného klíče.

Akce při přístupu – pro **povolení** nebo **zablokování** komunikace využívající daný certifikát bez ohledu na to, zda je důvěryhodný, vyberte možnost **Povolit** nebo Blokovat. V případě možnosti **Automaticky** budou důvěryhodné certifikáty povoleny, a v případě nedůvěryhodných bude muset uživatel vybrat akci. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Akce při **Kontrole** – pro **kontrolu** nebo **ignorování** komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém

režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – certifikát můžete přidat ručně ve formátu .cer, .crt nebo .pem a to buď přímo ze souboru nebo externího zdroje po zadání URL.

Změnit – vyberte certifikát, který chcete konfigurovat a klikněte na **Změnit**.

Odstranit – vyberte certifikát, který chcete smazat a klikněte na tlačítko **Odstranit**.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

Šifrovaná síťová komunikace

Pokud je váš systém nakonfigurován tak, aby kontroloval SSL/TLS, zobrazí se dialogové okno s výzvou k výběru akce ve dvou situacích:

Webová stránka používá neověřený nebo neplatný certifikát a ESET Endpoint Security je nakonfigurován tak, aby se dotázal uživatele (standardně je tato možnost aktivní pro neověřené certifikáty, nikoli neplatné), zda chcete komunikaci **Povolit** nebo **Zakázat**. Pokud se certifikát nenachází v Trusted Root Certification Authorities store (TRCA), je považován za nedůvěryhodný.

Za druhé, pokud je **režim SSL/TLS** nastaven na **Interaktivní**, zobrazí se u každé webové stránky dialogové okno s dotazem, zda se má komunikace **Kontrolovat** nebo**Ignorovat**. Některé aplikace ověřují, že jejich SSL nikdo nemodifikuje ani nekontroluje, v takových případech musí ESET Endpoint Security tuto komunikaci **ignorovat**, aby aplikace fungovala.

> **Názorné příklady**
> Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
> • Upozornění na certifikát v produktu ESET pro Windows
> • Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"

V obou případech je dostupná možnost pro zapamatování vybrané akce. Zapamatované akce jsou uloženy v Pravidlech pro certifikáty.

Ochrana poštovních klientů

Chcete-li nastavit Ochranu poštovních klientů, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** a vyberte jednu z následujících možností:

- Ochrana transportu zpráv
- Ochrana poštovní schránky
- Správa seznamů adres
- ThreatSense

Ochrana transportu zpráv

POP3(S) a IMAP(S) jsou nejrozšířenější protokoly určené pro příjem e-mailové komunikace prostřednictvím poštovního klienta. Internet Message Access Protocol (IMAP) je další internetový protokol pro získávání pošty. IMAP má oproti POP3 několik výhod, například více klientů se může současně připojit ke stejné poštovní schránce a udržovat informace o stavu zprávy (např. zda byla zpráva přečtena, zda na ni bylo odpovězeno nebo byla odstraněna. Modul ochrany poskytující tuto kontrolu je automaticky zaveden při spuštění systému a je pak aktivní v paměti.

ESET Endpoint Security poskytuje ochranu těchto protokolů bez ohledu na použitého e-mailového klienta a bez nutnosti změny konfigurace e-mailového klienta. Ve výchozím nastavení se kontroluje veškerá komunikace využívající protokoly POP3 a IMAP, bez ohledu na výchozí čísla portů POP3 / IMAP.
Protokol MAPI není kontrolován. Komunikace s Microsoft Exchange serverem však může být kontrolována po integrování modulu do e-mailového klienta, jako je Microsoft Outlook.

ESET Endpoint Security rovněž podporuje kontrolu protokolů IMAPS (585, 993) a POP3S (995), které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Endpoint Security kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Šifrovaná komunikace se standardně nekontroluje. Chcete-li zobrazit nastavení skeneru, otevřete Rozšířená nastavení > **Ochrany** > SSL/TLS.

Chcete-li nakonfigurovat ochranu přenosu pošty, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana transportu zpráv**.

Povolit ochranu transportu zpráv – pokud je tato ochrana povolena, bude ESET Endpoint Security kontrolovat poštovní komunikaci.

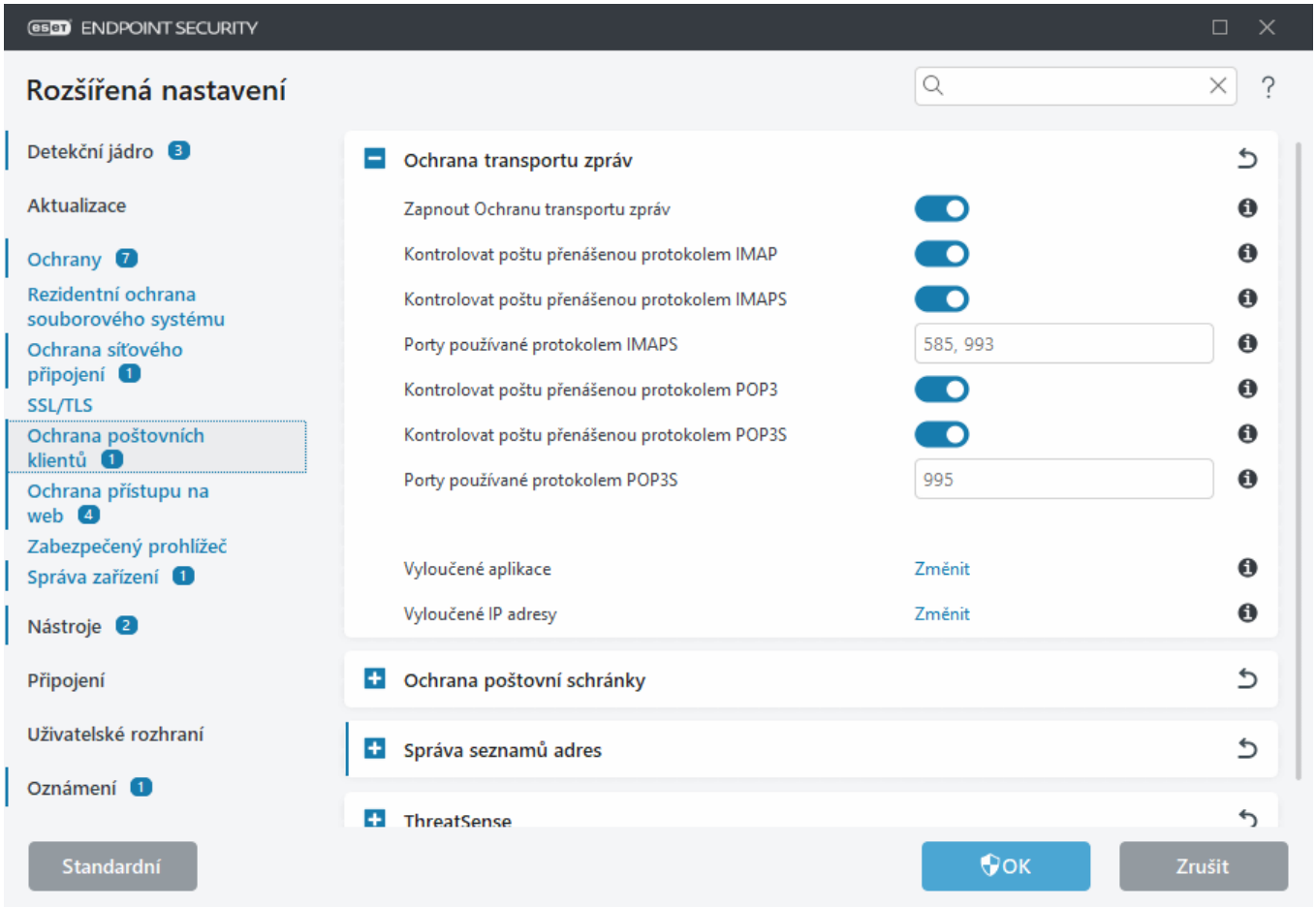
Kliknutím na přepínač vedle následujících možností můžete zvolit, které protokoly pro přenos pošty budou kontrolovány (ve výchozím nastavení je povolena kontrola všech protokolů):

- **Kontrolovat poštu přenášenou protokolem IMAP**
- **Kontrolovat poštu přenášenou protokolem IMAPS**
- **Kontrolovat poštu přenášenou protokolem POP3**
- **Kontrolovat poštu přenášenou protokolem POP3S**

Ve výchozím nastavení bude ESET Endpoint Security kontrolovat komunikaci na standardních portech IMAPS a POP3S. Chcete-li přidat vlastní porty pro protokoly IMAPS a POP3S, zadejte je do textového pole vedle **Porty používané protokolem IMAPS** nebo **Porty používané protokolem POP3S**. Více čísel portů je třeba oddělit čárkou.

Vyloučené aplikace – umožňuje neprovádět Ochranu poštovního transportu u zvolených aplikací. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

Vyloučené IP adresy – umožňuje neprovádět u konkrétních adres kontrolu pomocí Ochrany transportu zpráv. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



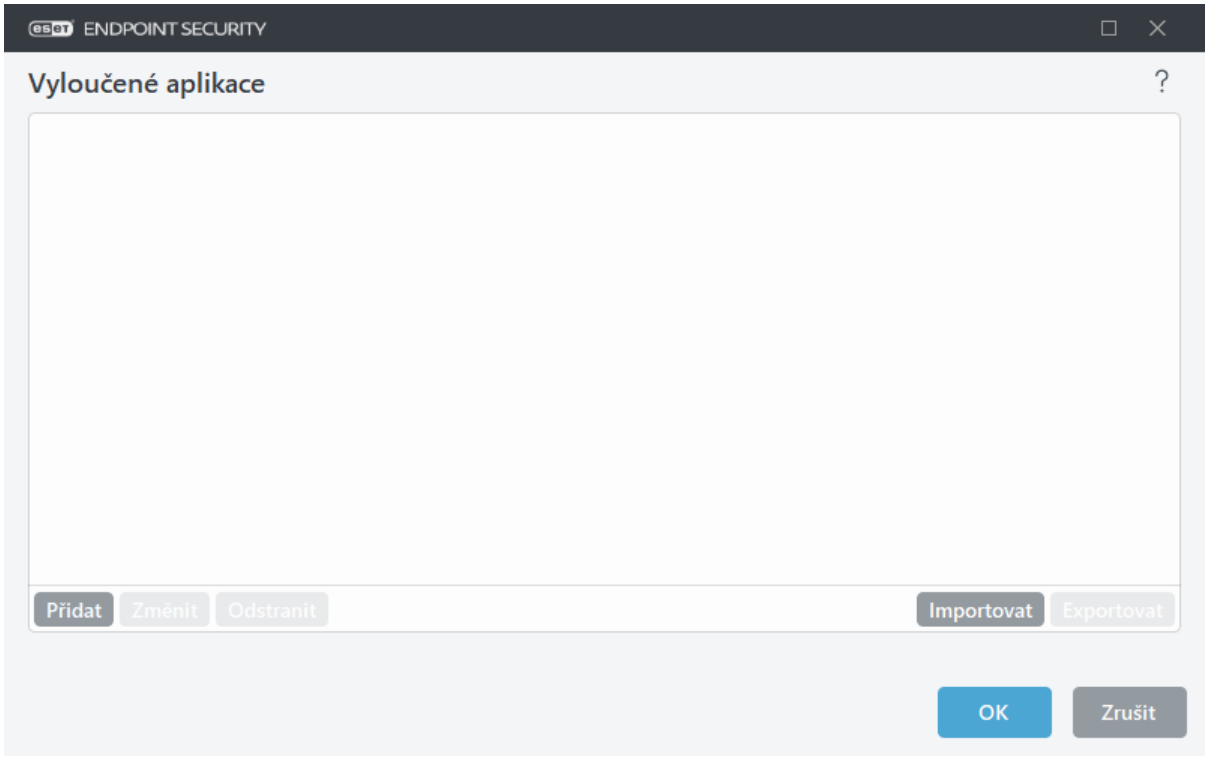
Vyloučené aplikace

Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu. HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na **...** a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



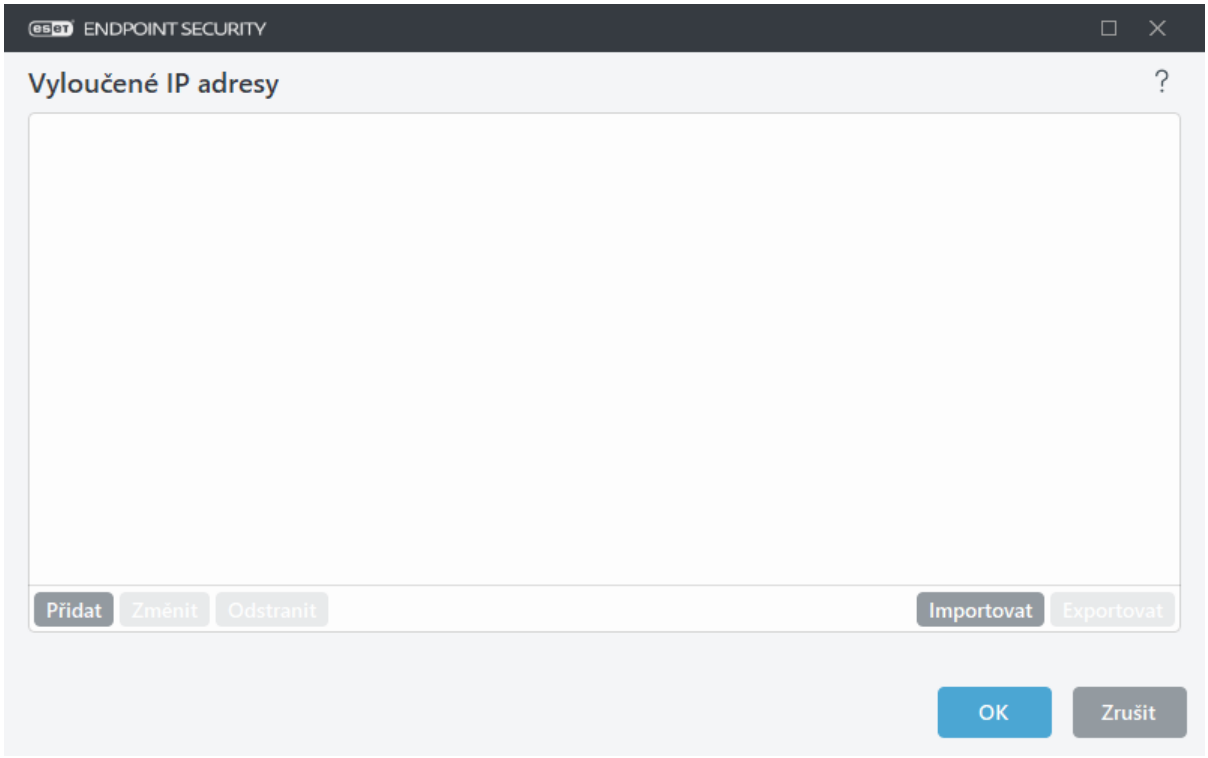
Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany, kterou chcete vyloučit z filtrování.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).

Rozsah adres – umožní zadat počáteční a koncovou IP adresu pro rozsah IP několika zařízení (například *192.168.0.1-192.168.0.99*).

Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsíť 192.168.1.0. Chcete-li vyloučit celou podsíť, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsíť – podsíť skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Ochrana poštovní schránky

Integrace ESET Endpoint Security s poštovní schránkou zvyšuje úroveň ochrany před škodlivým kódem v e-mailových zprávách.

Chcete-li nakonfigurovat ochranu poštovní schránky, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky**.

Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta – Vypnutím se deaktivuje ochrana zajišťovaná doplňkem v e-mailových klientech.

Vyberte e-maily pro kontrolu:

- **Příchozí zprávy**
- **Odchozí zprávy**
- **Čtené zprávy**
- **Změněná zpráva**

Doporučujeme, abyste možnost **Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta** měli zapnutou. I když integrace není zapnuta nebo je nefunkční, ochrana e-mailová komunikace je stále zajišťována prostřednictvím modulu Ochrana transportu zpráv (IMAP/IMAPS a POP3/POP3S).

Vyhledávání spamu

V současnosti mezi největší problémy e-mailové komunikace patří nevyžádaná pošta. Spam představuje více než 30 % veškeré e-mailové komunikace. Antispamovová ochrana poštovních klientů chrání před tímto problémem. Kombinuje několik principů zabezpečení e-mailů a poskytuje vynikající filtrování, aby vaše doručená pošta zůstala čistá. Pro detekci spamu je jedním z důležitých principů rozpoznávání nevyžádaných e-mailů na základě předdefinovaných důvěryhodných adres (povolených) a spamových adres (blokovaných).

Hlavním principem je rozpoznávání spamu na základě vlastností e-mailových zpráv. Přijatá zpráva je prověřena na základě pravidel (vzorky zpráv, statistická heuristika, rozpoznávací algoritmy a další jedinečné metody) a podle výsledku se rozhodně, zda se jedná o spam nebo ne.

Povolit Antispamovou ochranu poštovních klientů – pokud je tato funkce povolena, budou přijaté zprávy kontrolovány na přítomnost spamu.

Použít pokročilou kontrolu spamu – pravidelně se budou stahovat další antispamová data, čímž se zvyšují antispamové schopnosti a dosahuje se lepších výsledků.

Zapisovat skóre antispamové ochrany do protokolu – antispamové jádro ESET Endpoint Security přiřazuje každé zkontrolované zprávě skóre. Zpráva je zároveň zaznamenána do protokolu antispamové ochrany, který je dostupný v hlavním okně programu na záložce **Nástroje** > **Protokoly** > **Antispamovová ochrana poštovních klientů**.

- **Nezapisovat** – sloupec Skóre bude v protokolu antispamové ochrany prázdný.
- **Zapisovat pouze pro přehodnocené zprávy a zprávy označené jako SPAM** – vyberte tuto možnost, pokud chcete zapisovat spam skóre pouze pro zprávy označené jako SPAM.
- **Zapisovat pro všechny zprávy** – všechny zprávy budou mít zaznamenáno spam skóre.

Po kliknutí pravým tlačítkem na zprávu umístěnou ve složce spam můžete z kontextového menu vybrat možnost **Přehodnotit vybrané zprávy jako NENÍ spam**. Zpráva bude přemístěna do složky s doručenou poštou. Po kliknutí pravým tlačítkem na zprávu umístěnou ve složce doručené pošty můžete z kontextového menu vybrat možnost **Přehodnotit vybrané zprávy jako spam**. Zpráva bude přemístěna do složky s nevyžádanou poštou. Můžete vybrat více zpráv a provést akci na všech z nich současně.

Integrace – umožňuje integrovat Ochranu poštovní schránky do e-mailového klienta. Další informace naleznete v kapitole Integrace.

Reakce – umožňuje přizpůsobit zpracování nevyžádaných zpráv. Další informace naleznete v kapitole Reakce.

Integrace

Integrace ESET Endpoint Security do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdrženým prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET Endpoint Security

podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET Endpoint Security do poštovního klienta, což přispívá k efektivnější kontrole e-mailových zpráv. Chcete-li upravit nastavení integrace, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Integrace**.

Povolit integraci s Microsoft Outlook – Microsoft Outlook je v současné době jediným podporovaným e-mailovým klientem. Poštovní ochrana je zajišťována pomocí doplňku. Hlavní výhodou doplňku je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Úplný seznam podporovaných poštovních klientů a jejich verzí naleznete v ESET Databázi znalostí (článek nemusí být dostupný ve všech jazycích).

Pokročilé zpracování poštovními klienty – zpracovává další Outlook Messaging API (MAPI) události: Objekt upraven (`fnevObjectModified`) a Objekt vytvořen (`fnevObjectCreated`). Tuto možnost vypněte, pokud pozorujete propad výkonu při práci s vaším poštovním klientem.

Panel nástrojů v MS Outlook

Ochrana Microsoft Outlook pracuje jako zásuvný modul (plug-in). Po instalaci ESET Endpoint Security se do aplikace Microsoft Outlook přidá tento panel nástrojů s možnostmi antivirové ochrany a antispamové ochrany poštovních klientů:

Spam – umožňuje vybrané zprávy označit jako spam. Po označení se odešle "otisk" zprávy na centrální server s databází charakteristik nevyžádané pošty. V případě, že stejný "otisk" odešle větší počet uživatelů, bude tato zpráva v budoucnu vyhodnocena jako spam.

Není spam – umožňuje vybrané zprávy označit jako není spam.

Spamová adresa (seznam spamových adres, tzv. blacklist) – přidá adresu odesílatele na seznam spamových adres jako Blokováno. Všechny zprávy přijaté z těchto adres budou automaticky označovány jako spam.

> ⚠ Při odesílání nevyžádané pošty se využívá tzv. spoofing, kdy se skutečný odesílatel maskuje za jinou e-mailovou adresu. Buďte tedy obezřetní.

Důvěryhodná adresa (Povoleno, seznam důvěryhodných adres, tzv. whitelist) – přidá adresu odesílatele vybraných zpráv na Seznam důvěryhodných adres jako Povoleno. Zprávy z těchto adres nebudou nikdy automaticky označované jako spam.

ESET Endpoint Security – dvojitým kliknutím na ikonu otevřete hlavní okno programu ESET Endpoint Security.

Znovu zkontrolovat zprávy – umožní ruční spuštění kontroly e-mailů. V této části můžete vybrat zprávy, které budou zkontrolovány. Tím můžete aktivovat opakovanou kontrolu přijatého e-mailu. Další informace naleznete v kapitole Ochrana poštovní schránky.

Nastavení skeneru – zobrazí možnosti nastavení Ochrany poštovní schránky.

Nastavení antispamu – zobrazí možnosti nastavení ochrany poštovní schránky.

Antispamový seznam adres – otevře okno Správa seznamů adres, kde máte přístup k seznamům vyloučených, důvěryhodných a spamových adres.

Potvrzovací dialog

Dialog s možností potvrzení nebo zamítnutí dané akce slouží pro ověření, že chcete akci opravdu provést. Předejdete tím také akcím, jejichž provedení jste nastavili nedopatřením.

Zároveň můžete tato upozornění vyžadující potvrzení zcela vypnout.

Opakovaná kontrola zpráv

Na panelu nástrojů produktu ESET Endpoint Security integrovaném v poštovním klientovi máte k dispozici možnosti pro kontrolu zpráv. Dostupné jsou dvě možnosti kontroly:

Všechny zprávy v aktuální složce – zkontrolují se všechny zprávy ve složce, která je aktuálně zobrazena.

Pouze označené zprávy – zkontrolují se pouze zprávy, které jste vybrali ručně.

Možnost **Kontrolovat zprávy, které již byly překontrolovány** zajistí nové zkontrolování zpráv, které již byly v minulosti zkontrolovány.

Reakce

Na základě výsledků kontroly zpráv může ESET Endpoint Security zkontrolované zprávy přesunout nebo přidat vlastní text do předmětu. Tato nastavení můžete nakonfigurovat v Rozšířeném nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Reakce**.

Antispamovová ochrana poštovních klientů v ESET Endpoint Security umožňuje konfigurovat následující parametry zpráv:

Přidávat text do předmětu zprávy – umožňuje přidávat vlastní text do předmětu e-mailové zprávy klasifikované jako spam. Výchozí **text** je "[SPAM]".

Přesunout do spamové složky – po zapnutí této možnosti budou nevyžádané zprávy přesouvány do výchozí složky s nevyžádanou poštou a naopak, zprávy nevyhodnocené jako spam budou přesouvány do složky s doručenou poštou. Klikem pravým tlačítkem myši na e-mail a výběrem ESET Endpoint Security z kontextového menu můžete rovněž vybrat, jaké povahy pošta je.

Přesunout do vlastní složky – pokud je tato možnost povolena, budou nevyžádané zprávy přesunuty do níže uvedené složky.

Složka – definujte vlastní složku, do které přesouvat infikované zprávy.

Pokud zpráva obsahuje detekci, ve výchozím nastavení se ji ESET Endpoint Security pokusí vyléčit. Pokud zprávu nelze vyléčit, můžete zvolit **Akce, pokud není možné objekt vyléčit**:

- **Žádná akce** – program upozorní na zprávy s infikovanými přílohami, avšak neprovede žádnou akci.
- **Odstranit zprávu** – program upozorní na infikované přílohy a odstraní celou zprávu.
- **Přesunout zprávu do složky s odstraněnými zprávami** – program bude přesouvat infikované zprávy do složky s vymazanými zprávami.
- **Přesunout zprávu do složky** (výchozí akce) – program bude přesouvat infikované zprávy do vybrané složky.

Složka – definujte vlastní složku, do které přesouvat infikované zprávy.

Označit SPAM zprávy jako přečtené – po aktivování této možnosti se nevyžádaná zpráva označí jako přečtená. To vám pomůže koncentrovat pozornost na legitimní "čisté" doručené zprávy.

Přehodnocené zprávy označit jako nepřečtené – zprávy, které byly dříve označeny jako spam, budou po novém vyhodnocení jako legitimní označeny jako nepřečtené.

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do příchozích a čtených zpráv** nebo **Přidávat do odchozích zpráv**. Samozřejmě, na tyto podpisy se nelze zcela spoléhat, protože nemusí být doplněny do problematických HTML zpráv a také mohou být zfalšovány malwarem. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy nebo pro oboje. K dispozici jsou následující možnosti:

- **Nikdy** – program nebude přidávat podpisy,
- **Při výskytu detekce** – pouze zprávy obsahující škodlivý software budou označeny jako zkontrolované (výchozí).
- **Přidávat do všech kontrolovaných zpráv** – program bude přidávat zprávy do všech kontrolovaných e-mailů.

Modifikovat předmět příchozích a čtených zpráv / **Modifikovat předmět odchozích zpráv** – povolením této možnosti přidáte do zprávy vlastní text zadaný níže.

Šablona přidávaná do předmětu infikovaných zpráv – upravte tuto šablonu, pokud chcete změnit formát předpony předmětu infikovaného e-mailu. Tato funkce přidá k původnímu předmětu zprávy "Ahoj" předponu "[detekce %DETECTIONNAME%]". Proměnná %DETECTIONNAME% představuje detekovanou hrozbou.

Správa seznamů adres

Antispamová ochrana poštovních klientů v ESET Endpoint Security umožňuje nastavit různé parametry pro práci se seznamem adres. Chcete-li nakonfigurovat seznamy adres, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Správa seznamů adres**.

Povolit uživatelský seznam adres – pomocí této možnosti povolíte na tomto zařízení používání uživatelského seznamu adres.

Uživatelský seznam adres – po kliknutí na Změnit se zobrazí editor pravidel antispamové ochrany. Pravidla definovaná v tomto seznamu jsou platná pro aktuálně přihlášeného uživatele.

Povolit globální seznam adres – pomocí této možnosti povolíte používání globálního seznamu adres, který bude sdílený se všemi uživateli na tomto zařízení.

Globální seznam adres – po kliknutí na Změnit se zobrazí editor pravidel antispamové ochrany. Pravidla definovaná v tomto seznamu se aplikují na všechny uživatele.

Automatické povolení a přidávání do uživatelského seznamu adres

Považovat adresy ze seznamu kontaktů za důvěryhodné – pokud je tato možnost aktivní, adresy z vašeho seznamu kontaktů budou považovány za důvěryhodné, aniž by se nacházely na uživatelském seznamu adres.

Přidávat adresy příjemců z odesílaných zpráv – po aktivování této možnosti se na seznam povolených adres

přidají všechny adresy příjemců, kterým jste zaslali e-mail.

Přidávat adresy odesílatelů ze zpráv klasifikovaných jako NENÍ SPAM – po aktivování této možnosti se na seznam povolených adres přidají adresy odesílatelů zpráv, které byly přehodnocené jako NENÍ SPAM.

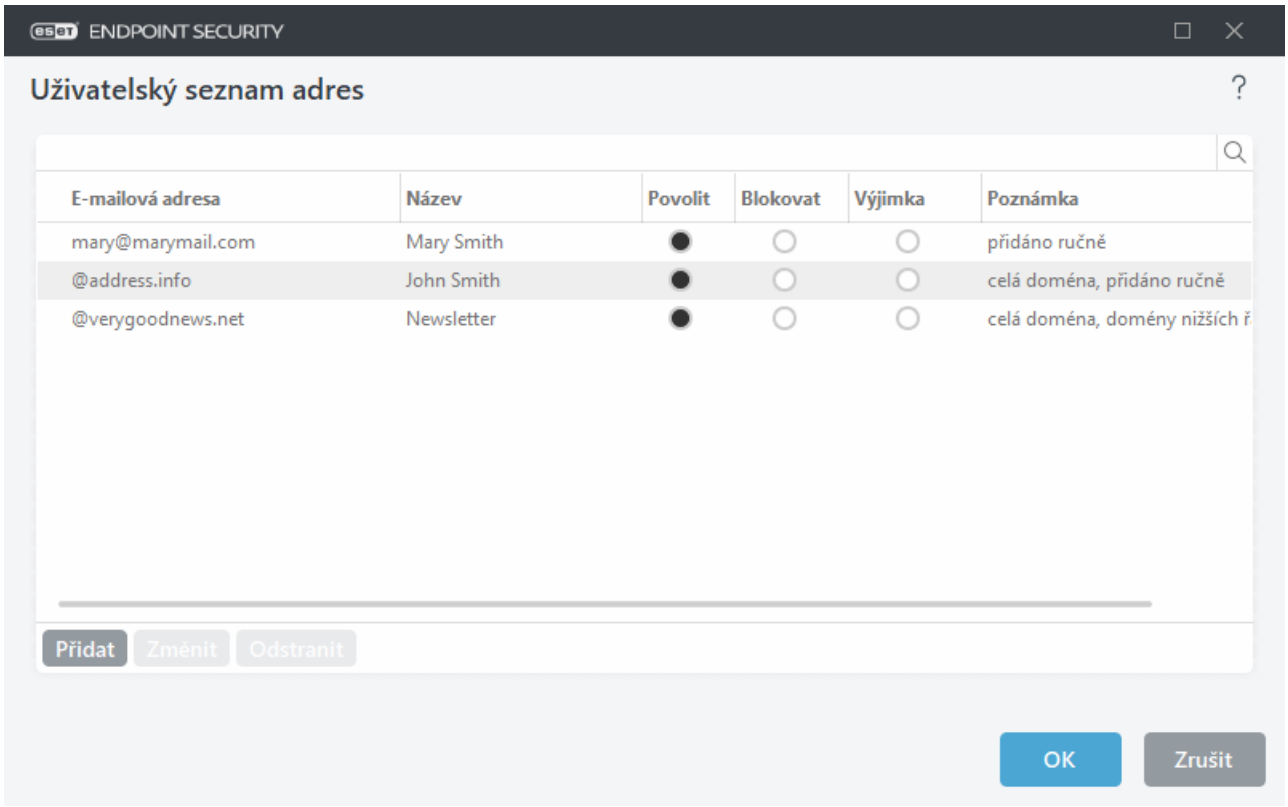
Automatické přidávání do uživatelského seznamu adres jako výjimky

Přidávat adresy z vlastních účtů – umožní přidání e-mailových adres z poštovního klienta do uživatelského seznamu adres jako výjimky.

Seznamy adres

Pro zajištění ochrany před nevyžádanými e-maily vám ESET Endpoint Security umožňuje definovat seznamy e-mailových adres.

Chcete-li upravit seznamy adres, otevřete Rozšířená nastavení > **Ochrany** > **Ochrana poštovních klientů** > **Správa seznamů adres** a klikněte na tlačítko **Změnit** vedle položky **Uživatelský seznam adres** nebo **Globální seznam adres**.



Sloupce

E-mailová adresa – adresa, na kterou se bude pravidlo vztahovat.

Název pravidla – název vámi definovaného pravidla.

Povolit/Blokovat/Výjimka – pole používaná k určení, jakou akci provést pro e-mailovou adresu (kliknutím na pole v upřednostňovaném sloupci akci rychle změníte):

- **Povolit** – Adresy, které považujete za důvěryhodné a chcete z nich vždy dostávat e-maily.
- **Blokovat** – Adresy, které považujete za nedůvěryhodné/spam a ze kterých nechcete dostávat e-maily.
- **Výjimka** – Adresy, které jsou vždy kontrolovány pro možný výskyt spamové pošty a které mohou být zfalšovány a použity pro jeho odesílání.

Poznámka – informace o tom, kým bylo pravidlo vytvořeno, a zda se vztahuje na celou doménu / domény nižší úrovně.

Správa adres

- **Přidat** – kliknutím přidáte pravidlo pro novou adresu.
- **Změnit** – kliknutím upravíte existující pravidlo.
- **Odstranit** – kliknutím odstraníte existující pravidlo ze seznamu.

Přidat/Upravit záznam

Toto okno umožňuje přidat nebo upravit adresu ve Správě seznamů adres a definovat akci, která se má provést:

E-mailová adresa – adresa, na kterou se bude pravidlo vztahovat. Zástupné znaky nejsou podporovány.

Název pravidla – název vámi definovaného pravidla.

Akce – Akce, která se má provést, pokud se e-mailová adresa kontaktu shoduje s adresou zadanou v poli **E-mailová adresa**:

- **Povolit** – Adresy, které považujete za důvěryhodné a chcete z nich vždy dostávat e-maily.
- **Blokovat** – Adresy, které považujete za nedůvěryhodné/spam a ze kterých nechcete dostávat e-maily.
- **Výjimka** – Adresy, které jsou vždy kontrolovány pro možný výskyt spamové pošty a které mohou být zfalšovány a použity pro jeho odesílání.

Celá doména – vybráním této možnosti se do seznamu zařadí celá doména daného kontaktu (ne jen **konkrétní e-mailová adresa**, ale všechny e-mailové adresy z domény například z *adresa.cz*).

Domény nižších řádů – vybráním této možnosti se do seznamu zařadí doména nižších řádů daného kontaktu (*adresa.cz* reprezentuje doménu, zatímco *moje.adresa.cz* subdoménu).

Výsledek zpracování adres

Při přidávání nebo přesouvání e-mailových adres mezi seznamy povolených adres, spamových adres a seznamem výjimek může ESET Endpoint Security zobrazit oznámení. Obsah oznámení závisí na akci, kterou jste se pokoušeli provést.

Vybráním možnosti **Příště tuto zprávu nezobrazovat** se akce provede automaticky a okno se již příště nezobrazí.

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci

několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v Rozšířeném nastavení pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochran kromě Kontroly počítače.

Kontrolované objekty

V této sekci můžete vybrat součásti počítače a soubory, které budou testovány na přítomnost infiltrace.

Operační paměť – kontrola přítomnosti hrozeb, které mohou být zavedeny v operační paměti počítače.

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do slovníku pojmů.

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

Archivy – podporovány jsou formáty ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE (Outlook Express) a soubory.

Samorozbalovací archivy – archivy které nepotřebují pro své rozbalení jiné programy. Jedná se o SFX (Self-extracting) archivy.

Runtime archivy – runtime archivy se na rozdíl od klasických archivů po spuštění rozbalí v paměti počítače. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG aj.) program podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

Rozšířená heuristika/DNA/Smart vzorky – rozšířená heuristika se skládá z unikátních heuristických algoritmů vyvinutých společností ESET optimalizovaných pro detekci počítačových červů a trojských koňů napsaných ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopni produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých škodlivých kódů.

Léčení

Nastavení léčení ovlivňuje chování ESET Endpoint Security během léčení objektů.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci detekčního jádra ThreatSense pro volitelnou kontrolu počítače jsou v části **Ostatní** k dispozici také následující možnosti:

Kontrolovat alternativní datové proudy (ADS) – alternativní datové proudy používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho infiltrací je proto využívá jako maskování před případným odhalením.

Spustit kontrolu na pozadí s nízkou prioritou – každá kontrola počítače využívá určité množství systémových zdrojů. Pokud právě pracujete s programy náročnými na výkon procesoru, přesunutím kontroly na pozadí jí můžete přiřadit nižší prioritu a získat více prostředků pro ostatní aplikace.

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do protokolu zapíší všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnuté Smart optimalizaci je použito nejoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena. V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány. Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik). Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: 3 GB.

> Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Ochrana přístupu na web

Ochrana přístupu na web umožňuje konfigurovat pokročilá nastavení modulu Internetová ochrana. V Rozšířeném nastavení > **Ochrany** > **Ochrana přístupu na web** > **Ochrana přístupu na web** jsou k dispozici následující možnosti:

Zapnout ochranu přístupu na web – pokud je tato možnost vypnutá, nefunguje Ochrana přístupu na web ani Anti-Phishingová ochrana.

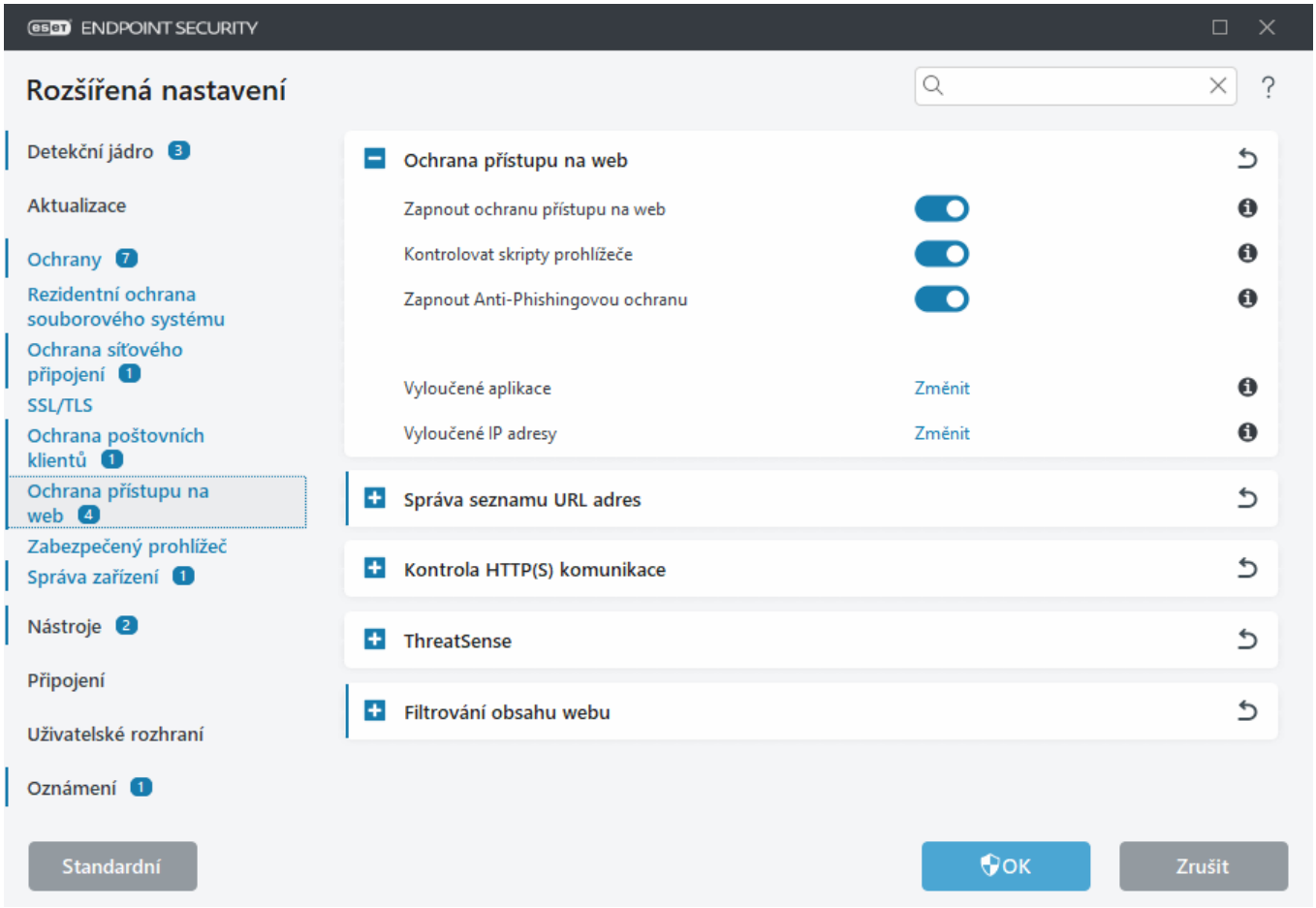
> Důrazně doporučujeme ponechat Ochranu přístupu na web zapnutou a nevylučovat žádné aplikace ani IP adresy ve výchozím nastavení.

Kontrolovat skripty prohlížeče – pokud je tato funkce povolena, detekční jádro zkontroluje všechny JavaScript programy spouštěné webovými prohlížeči.

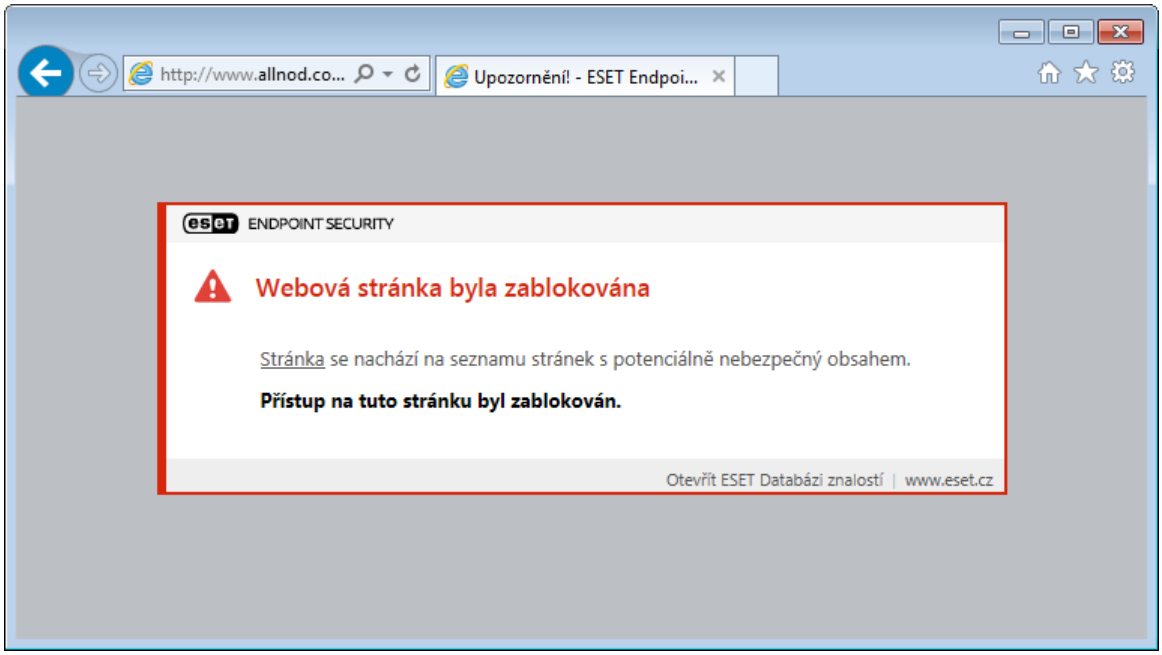
Zapnout Anti-Phishingovou ochranu – pokud je povolena, jsou phishingové webové stránky blokovány. Pro více informací přejděte do kapitoly Anti-Phishingová ochrana.

Vyloučené aplikace – umožňuje vyloučit konkrétní aplikace z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

Vyloučené IP adresy – umožňuje vyloučit konkrétní IP adresy z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



Při přístupu na blokovanou stránku se v internetovém prohlížeči zobrazí níže uvedená zpráva:



Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:

- Jak odblokovat přístup na bezpečnou stránku přímo v ESET Endpoint Security

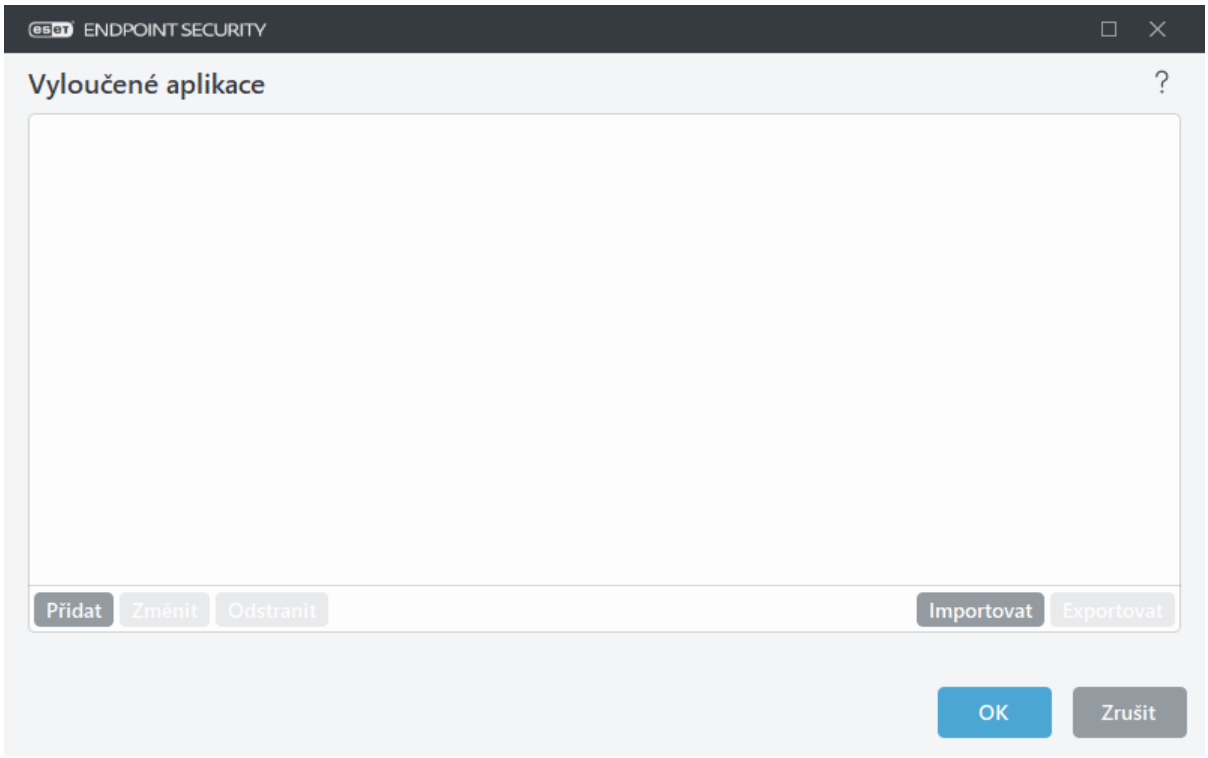
Vyloučené aplikace

Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu. HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na **...** a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



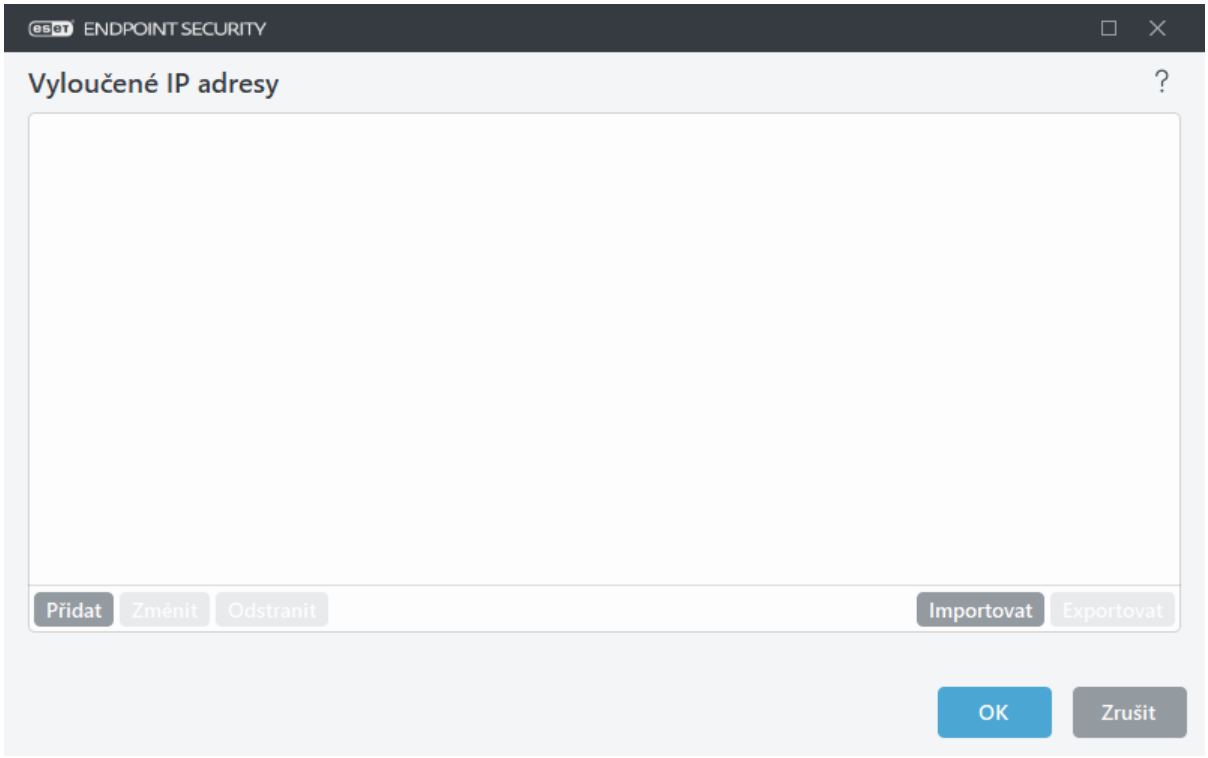
Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany, kterou chcete vyloučit z filtrování.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Příklady IP adres

Přidání IPv4 adresy:
Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).
Rozsah adres – umožní zadat počáteční a koncovou IP adresu pro rozsah IP několika zařízení (například *192.168.0.1-192.168.0.99*).
Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsíť 192.168.1.0. Chcete-li vyloučit celou podsíť, zadejte *192.168.1.0/24*.
Přidání IPv6 adresy:
Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podsíť – podsíť skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Správa seznamu URL adres

Správa seznamu URL adres v Rozšířeném nastavení > **Ochrany** > **Ochrana přístupu na web** umožňuje zadat HTTP adresy, které se mají blokovat, povolit nebo vyloučit z kontroly obsahu webu.

Pokud chcete filtrovat kromě HTTP adres kontrolovat také HTTPS adresy, musí být zapnutý protokol SSL/TLS. V opačném případě by byl zakázán pouze přístup na nešifrovanou HTTPS verzi webové stránky.

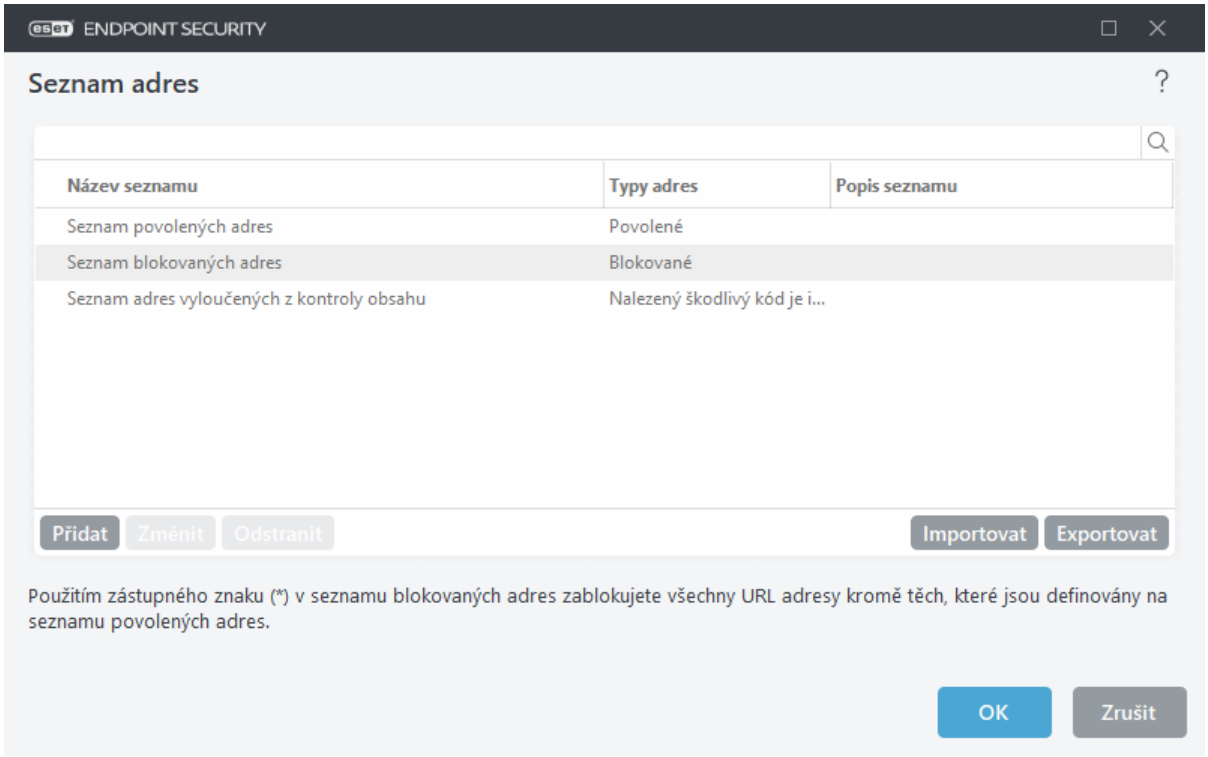
Webové stránky zařazené na **Seznamu blokovaných adres** nebudou dostupné, na rozdíl od adres uvedených na **Seznamu povolených adres**. Webové stránky zařazené na **Seznamu adres vyloučených z kontroly obsahu** nebudou kontrolovány na přítomnost škodlivého kódu.

Pokud chcete zablokovat všechny HTTP adresy kromě těch definovaných na **Seznamu povolených adres**, zadejte do již definovaného **Seznamu blokovaných adres** * (hvězdičku).

V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Adresy vyloučené z kontroly se nekontrolují na přítomnost hrozeb, proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Je potřeba dbát opatrnosti při

používání speciálních znaků v tomto seznamu. Pro více informací, jak bezpečně přidat celou doménu včetně jejich subdomén, přejděte do kapitoly Přidání masky adresy/domény. Pro aktivování seznamu vyberte možnost **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit zobrazení upozornění zaškrtnutím možnosti **Upozornit při aplikování adresy ze seznamu**.

> **Adresy důvěryhodné pro ESET**
> Pokud je povolena možnost **Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné**, nebudou tyto domény ovlivněny vámi vytvořeným seznamem URL adres.



Ovládací prvky

Přidat – umožňuje vytvořit nový seznam. To je užitečné, pokud chcete adresy rozdělit do logických skupin. Například jeden seznam blokovaných adres může obsahovat adresy z veřejných blacklistů, a druhý vámi definované adresy. V takovém případě je správa seznamu externích adres mnohem snadnější.

Změnit – kliknutím upravíte existující seznam adres. Tuto možnost použijte pro přidání nebo odebrání adres ze seznamu.

Odstranit – odebere existující seznam. Toto platí pouze na seznamy vytvořené ručně pomocí volby **Přidat**, nikoli předdefinované.

Seznam adres

V této části můžete zadat seznamy HTTP(S) adres, které budou blokovány, povoleny nebo vyloučeny z kontroly.

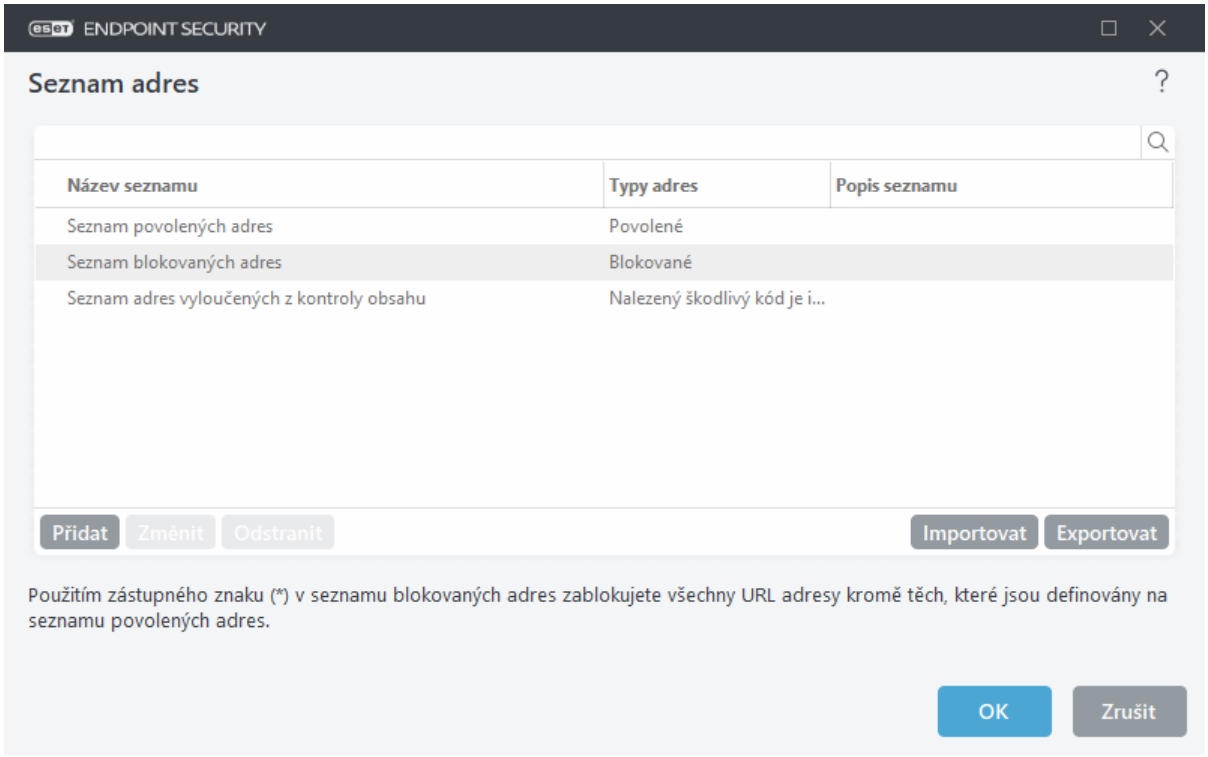
Standardně jsou k dispozici tři seznamy:

- **Seznam adres vyloučených z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na škodlivý kód.
- **Seznam povolených adres** – pokud do seznam blokovaných adres vložíte hvězdičku (*), bude uživateli

povolen přístup pouze na adresy uvedené v tomto seznamu. Přístup na tyto adresy bude povolen i v případě, že se zároveň nachází na seznamu blokovaných adres.

- **Seznam blokovaných adres** – na adresy uvedené v tomto seznamu nebude povolen přístup, pokud se zároveň nenachází na seznamu povolených adres.

Pro vytvoření nového seznamu klikněte na tlačítko **Přidat**. Pro odebrání seznamu klikněte na tlačítko **Odstranit**.



Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
- Jak odblokovat přístup na bezpečnou stránku přímo v ESET Endpoint Security

Pro více informací přejděte do kapitoly Správa URL adres.

Vytvoření nového seznamu URL adres

V tomto dialogovém okně můžete vytvořit nový seznam adres/masek, které budou blokovány, povoleny, nebo vyloučeny z kontroly.

Při vytváření nového seznamu jsou dostupné následující možnosti:

Typ seznamu adres – k dispozici jsou tři typy předdefinovaných seznamů:

- **Vyloučené z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na přítomnost škodlivého kódu.
- **Blokované** – na adresy v tomto seznamu nebude povolen přístup.
- **Povolené** – pokud do seznam blokovaných adres vložíte hvězdičku (*), bude uživateli povolen přístup pouze na adresy uvedené v tomto seznamu. Přístup na tyto adresy bude povolen i v případě, že se zároveň nachází na seznamu blokovaných adres.

Název seznamu – zadejte název nového seznamu. Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.

Popis seznamu – zadejte krátký popis pro nově vytvářený seznam (nepovinné). Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.

Pro aktivaci seznamu vyberte možnost **Seznam je aktivní**. Pokud chcete být upozorněni při přístupu k adrese uvedené na seznamu, aktivujte možnost **Upozornit při přístupu na adresy ze seznamu**. V takovém případě se zobrazí oznámení o tom, že přistupujete na webovou stránku zařazenou na seznamu například blokovaných nebo povolených stránek. V oznámení se zobrazí název seznamu obsahujícího zadanou webovou stránku.

Zaznamenávat od úrovně – z rozbalovacího menu vyberte úroveň, od které chcete záznamy zapisovat do protokolu. Záznamy s úrovní Varování budou přenášeny do ESET PROTECT.

Možnosti nastavit úroveň pro zaznamenávání událostí do protokolu s hodnotou Informační a Varování je dostupná pouze v případě, kdy pravidlo obsahuje v rámci domény alespoň dvě komponenty bez zástupných znaků. Příklad:
- *.domain.com/*
- *www.domain.com/*

Ovládací prvky

Přidat – kliknutím přidáte na seznam novou URL adresu (pro hromadné přidání více hodnot použijte oddělovač).

Změnit – kliknutím upravíte existující záznam. Tato možnost je dostupná pouze nad hodnotami, které jste **přidali** ručně.

Odstranit – kliknutím odstraníte záznam ze seznamu. Tato možnost je dostupná pouze nad hodnotami, které jste **přidali** ručně.

Importovat – kliknutím můžete naimportovat adresy ze souboru (kdy je každá hodnota na novém řádku a jde například o *.txt v UTF-8 kódování).

Další informace naleznete v kapitole Jak přidat masku URL.

Jak přidat masku URL?

Před zadáním požadované masky adresy/domény se seznamte s instrukcemi.

ESET Endpoint Security umožňuje zablokovat přístup na specifické stránky a dokáže zabránit internetovému prohlížeči v zobrazení jejich obsahu. Dále umožňuje specifikovat adresy, které mají být vyloučeny z kontroly. Pokud neznáte celý název vzdáleného serveru, nebo chcete specifikovat celou skupinu vzdálených serverů, můžete použít tzv. masky. V tomto případě jsou povoleny speciální znaky ? a * přičemž:

- znak ? nahrazuje libovolný symbol,
- znak * nahrazuje libovolný textový řetězec.

Například *.c?m bude platit pro všechny adresy, jejichž poslední část adresy začíná znakem c, končí znakem m a uprostřed se nachází libovolný znak (.com, .cam apod.).

Například maska *x? představuje libovolnou adresu, kde předposledním znakem je "x". Pokud chcete v masce zahrnout celou doménu, použijte formát **.domain.com/**. Definování protokolu (*http://*, *https://*) v předponě masky není povinné. Pokud jej vynecháte, maska bude platná pro jakýkoli protokol. Pokud použijete "*." na začátku názvu domény, bude sekvence vyhodnocena odlišně. Zaprvé, zástupný znak hvězdičky ("*") v tomto

případě nenahrazuje lomítko ("/"). To proto, aby se například maska *.domena.cz nevyhodnocovala jako adresa http://jakakolidomena.cz/cesta#.domena.cz (jako přípona může být připojena k jakékoli URL adrese bez toho, že by došlo k zablokování stahování). Za druhé, v tomto zvláštním případě odpovídá "*." také prázdnému řetězci. Jedna maska tak může zahrnovat celou doménu, včetně jejích subdomén. Například maska *.domain.com se použije nejen pro vyhodnocení adresy http://domain.com. Nicméně použití masky *domena.cz je nesprávné, protože bude použita také pro vyhodnocení adresy http://jinadomena.cz.

Možnosti nastavit úroveň pro zaznamenávání událostí do protokolu s hodnotou Informační a Varování je dostupná pouze v případě, kdy pravidlo obsahuje v rámci domény alespoň dvě komponenty bez zástupných znaků. Příklad:
- *.domain.com/*
- *www.domain.com/*

Kontrola HTTP(S) komunikace

Ve výchozím nastavení je aplikace ESET Endpoint Security nakonfigurována tak, aby kontrolovala HTTP a HTTPS komunikaci, kterou používají internetové prohlížeče a další aplikace. Kontrolu komunikace byste měli zakázat pouze v případě, že máte problémy se softwarem třetí strany a chcete zjistit, zda tento problém způsobuje ESET Endpoint Security.

Zapnout kontrolu HTTP komunikace – HTTP komunikace je vždy kontrolována na všech portech pro všechny aplikace.

Zapnout kontrolu HTTPS komunikace – HTTPS komunikace používá k přenosu informací mezi serverem a klientem šifrovaný kanál. ESET Endpoint Security kontroluje komunikaci pomocí protokolů SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovat pouze komunikaci na portech definovaných v části **Porty používané protokolem HTTPS** bez ohledu na verzi operačního systému (k předdefinovaným portům 443 a 0-65535 můžete přidat další).

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v Rozšířeném nastavení pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu

- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochran kromě Kontroly počítače.

Kontrolované objekty

V této sekci můžete vybrat součásti počítače a soubory, které budou testovány na přítomnost infiltrace.

Operační paměť – kontrola přítomnosti hrozeb, které mohou být zavedeny v operační paměti počítače.

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do slovníku pojmů.

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

Archivy – podporovány jsou formáty ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE (Outlook Express) a soubory.

Samorozbalovací archivy – archivy které nepotřebují pro své rozbalení jiné programy. Jedná se o SFX (Self-extracting) archivy.

Runtime archivy – runtime archivy se na rozdíl od klasických archivů po spuštění rozbalí v paměti počítače. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG aj.) program podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

Rozšířená heuristika/DNA/Smart vzorky – rozšířená heuristika se skládá z unikátních heuristických algoritmů vyvinutých společností ESET optimalizovaných pro detekci počítačových červů a trojských koňů napsaných ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopni produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých škodlivých kódů.

Léčení

Nastavení léčení ovlivňuje chování ESET Endpoint Security během léčení objektů.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci detekčního jádra ThreatSense pro volitelnou kontrolu počítače jsou v části **Ostatní** k dispozici také následující možnosti:

Kontrolovat alternativní datové proudy (ADS) – alternativní datové proudy používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho infiltrací je proto využívá jako maskování před případným odhalením.

Spustit kontrolu na pozadí s nízkou prioritou – každá kontrola počítače využívá určité množství systémových zdrojů. Pokud právě pracujete s programy náročnými na výkon procesoru, přesunutím kontroly na pozadí jí můžete přiřadit nižší prioritu a získat více prostředků pro ostatní aplikace.

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do protokolu zapíší všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnuté Smart optimalizaci je použito nejoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena. V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány. Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální

velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik). Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: 3 GB.

Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

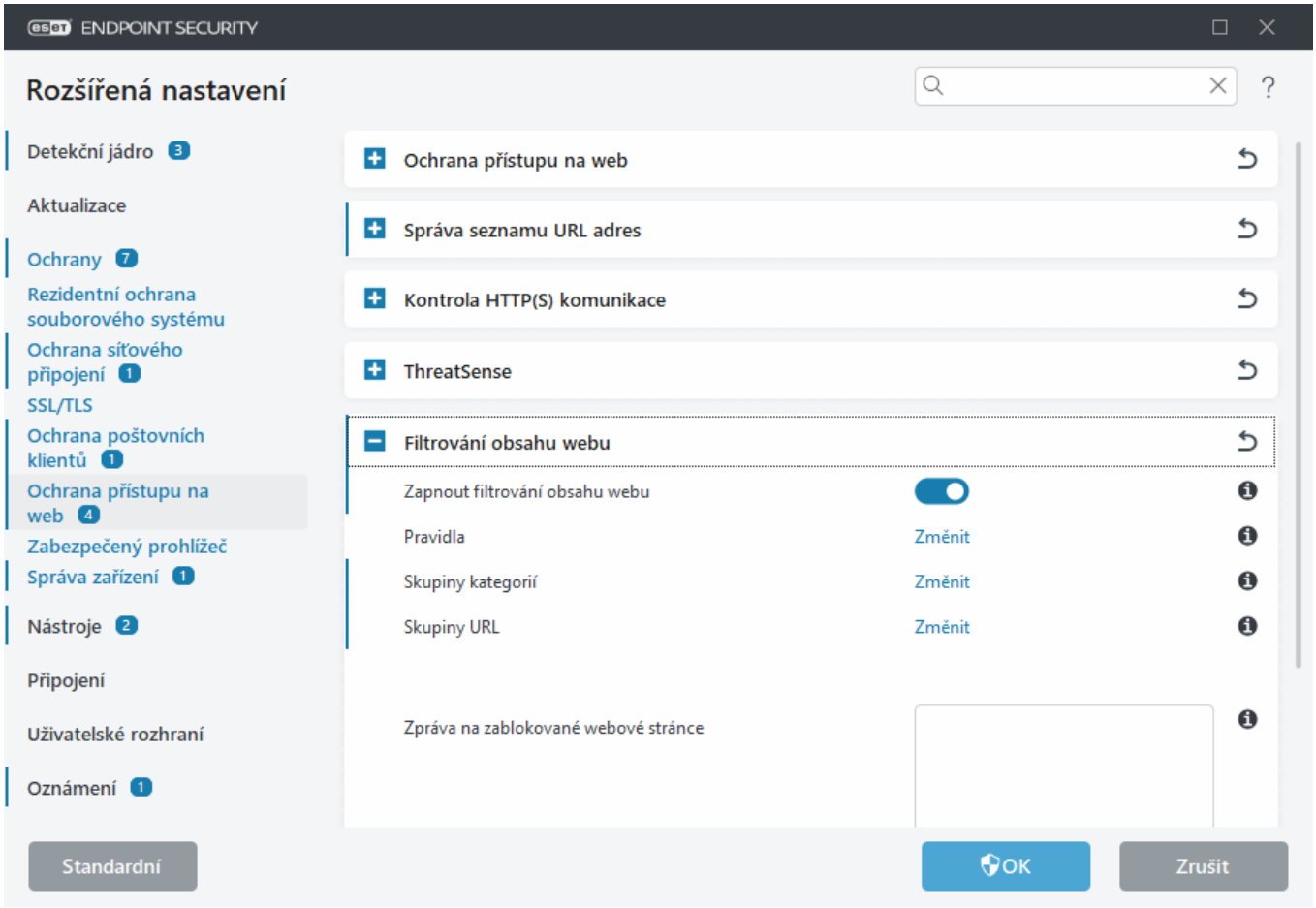
Filtrování obsahu webu

V sekci Filtrování obsahu webu naleznete nastavení, které vám pomůže ochránit firmu před rizikem právní zodpovědnosti. Prostřednictvím filtrování obsahu webu dokážete blokovat webové stránky, které mohou obsahovat potenciálně nevhodný obsah nebo mohou porušovat duševní vlastnictví jiných osob. Cílem je zabránit zaměstnancům v přístupu na tyto stránky, stejně tak stránky, které mohou negativně ovlivnit jejich produktivitu.

Filtrování obsahu webu umožňuje blokovat webové stránky s potenciálně urážlivým obsahem. Kromě toho můžete jako zaměstnavatel/administrátor zakázat přístup na 27 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

Standardně je Filtrování obsahu webu vypnuté. Pro aktivaci:

1. Otevřete Rozšířená nastavení > **Ochrany** > **Ochrana přístupu na web** > **Filtrování obsahu webu**.
2. Pomocí přepínače aktivujte možnost **Zapnout filtrování obsahu webu** v ESET Endpoint Security.
3. Nakonfigurujte přístup ke konkrétním webovým stránkám. Kliknutím na **Změnit** na řádku **Pravidla** získáte přístup k Editoru pravidel.

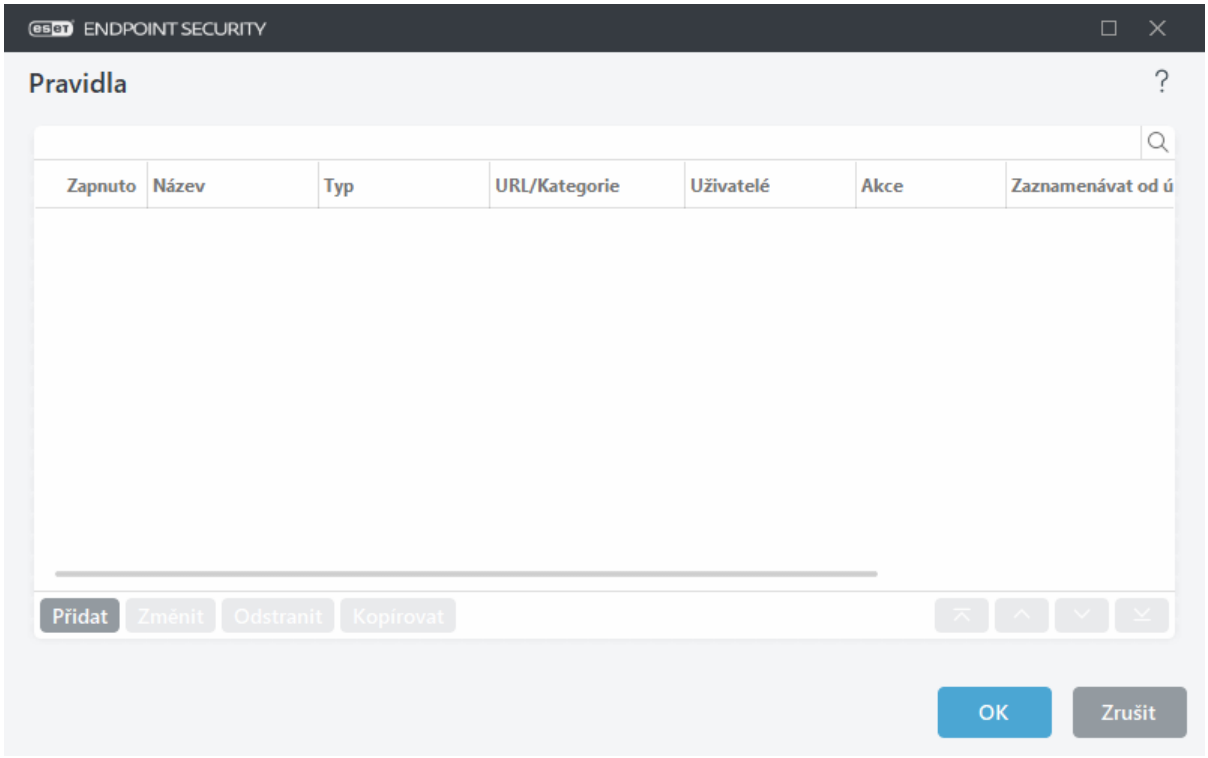


Pole **Zpráva na zablokované webové stránce** a **Obrázek na zablokované webové stránce** umožňují přizpůsobit zprávu, která se zobrazí u zablokované stánky.

> Pro zablokování přístupu na všechny webové stránky a povolení jen konkrétních využijte seznamy blokovaných/povolených adres.

Filtrování obsahu webu – pravidla

Editor pravidel zobrazuje existující pravidla pro URL adresy a kategorie webových stránek.



Seznam pravidel obsahuje některé popisy, jako např. název, typ blokování, akci, která se má provést při přístupu na danou stránku a úroveň protokolování.

Pro správu pravidel klikněte na tlačítko **Přidat** nebo **Změnit**. Stisknutím klávesy **CTRL** a kliknutím můžete vybrat více pravidel najednou a provést hromadné akce. Pomocí zaškrtávacího pole ve sloupci **Zapnuto** dané pravidlo zapnete nebo vypnete. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Pravidla jsou řazena v pořadí, ve kterém jsou vyhodnocována – pravidlo s nejvyšší prioritou je nahoře. Pro změnu priority vyberte požadované pravidlo a klikněte na odpovídající tlačítko se šipkou, v závislosti na tom, zda chcete prioritu zvýšit nebo snížit . Kliknutím na tlačítko s dvojitou šipkou přesunete pravidlo na začátek, resp. na konec seznamu.

Další informace naleznete také v kapitole věnované vytváření pravidel.

Přidání pravidla

V okně Pravidla filtrování obsahu webu můžete ručně vytvořit nebo upravit existující pravidlo filtrování obsahu webu.

Název

Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla.

Zapnuto

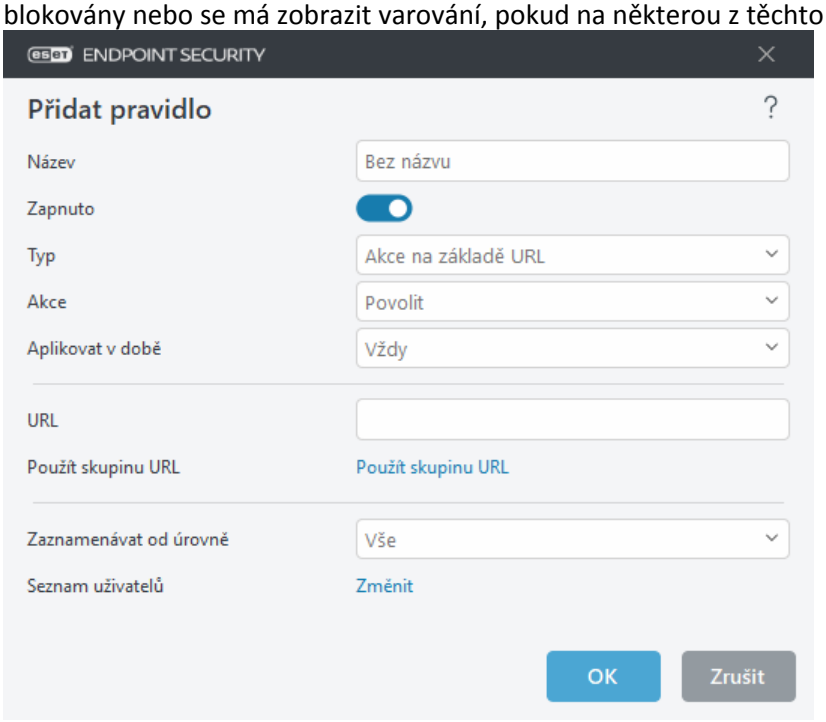
Pomocí možnosti **Zapnuto** dané pravidlo zapnete nebo vypnete. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Akce

Rozhodněte se, zda chcete pravidlo vytvářet na základě **URL** nebo **kategorie**.

Akce na základě URL

Pravidlo bude platné pro konkrétní stránku definovanou v poli **URL**.
V seznamech URL adres není možné používat zástupné znaky * (hvězdička) a ? (otazník). V případě adres s více doménami nejvyšší úrovně (TLD) je nutné jednotlivé TLD zadat do skupiny URL samostatně. Po vložení domény do skupiny bude veškerý obsah nacházející se na této doméně a všech subdoménách (například *sub.stranka.com*) blokován nebo povolen – na základě vámi definované akce.
URL nebo **Použít skupinu URL** – umožňuje zadat URL adresu nebo Skupinu URL, které mají být povoleny, blokovány nebo se má zobrazit varování, pokud na některou z těchto URL adres uživatel vstupuje.



Akce na základě kategorie

Pravidlo bude použito na základě kategorie webových stránek.
Kategorie URL nebo **Použít skupinu** – vyberte kategorii webových stránek nebo skupinu kategorií, které chcete povolit, zablokovat nebo varovat uživatele, když je zjištěna jedna z kategorií.

Přístupová oprávnění

- **Povolit** – přístup k URL adrese/kategorii je povolen.
- **Upozornit** – zablokuje přístup k URL adrese/kategorii. Kliknutím na **Vrátit se zpět** se můžete vrátit na předchozí webovou stránku nebo kliknutím na **Pokračovat** můžete webovou stánku otevřít. Pokud kliknete na **Pokračovat**, blokovací stránka se při příští návštěvě webu nezobrazí.
- **Vždy varovat** – zablokuje přístup k URL adrese/kategorii. Kliknutím na **Vrátit se zpět** se můžete vrátit na předchozí webovou stránku nebo kliknutím na **Pokračovat** můžete webovou stánku otevřít. Blokovací stránka se zobrazí při každé návštěvě této webové stránky.
- **Blokovat** – zablokuje přístup k URL adrese/kategorii. Kliknutím na **Vrátit se zpět** se můžete vrátit na předchozí webovou stránku.

Aplikovat v době

Umožňuje použít vytvořené pravidlo během určité doby. Vyberte vytvořený časový úsek z rozbalovacího menu **Aplikovat v době**. Pro více informací přejděte do kapitoly časové sloty.

Zaznamenávat do protokolu

- **Vždy** – do protokolu se zaznamená veškerá online komunikace.
- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů,
- **Informační** – zaznamenány budou informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíší kritické chyby a varovná hlášení.
- **Žádné** – nezaznamenají se žádné informace.

> Úroveň protokolování můžete nastavit jednotlivě pro každý seznam. Do ESET PROTECT se budou odesílat události s úrovní **Varování**.

Seznam uživatelů

- **Přidat** – otevře dialogové okno **Seznam uživatelů nebo skupin** pro výběr požadovaných uživatelů. Pokud není vybrán žádný uživatel, pravidlo se použije pro všechny uživatele.
- **Odstranit** – odebere vybraného uživatele z filtru.

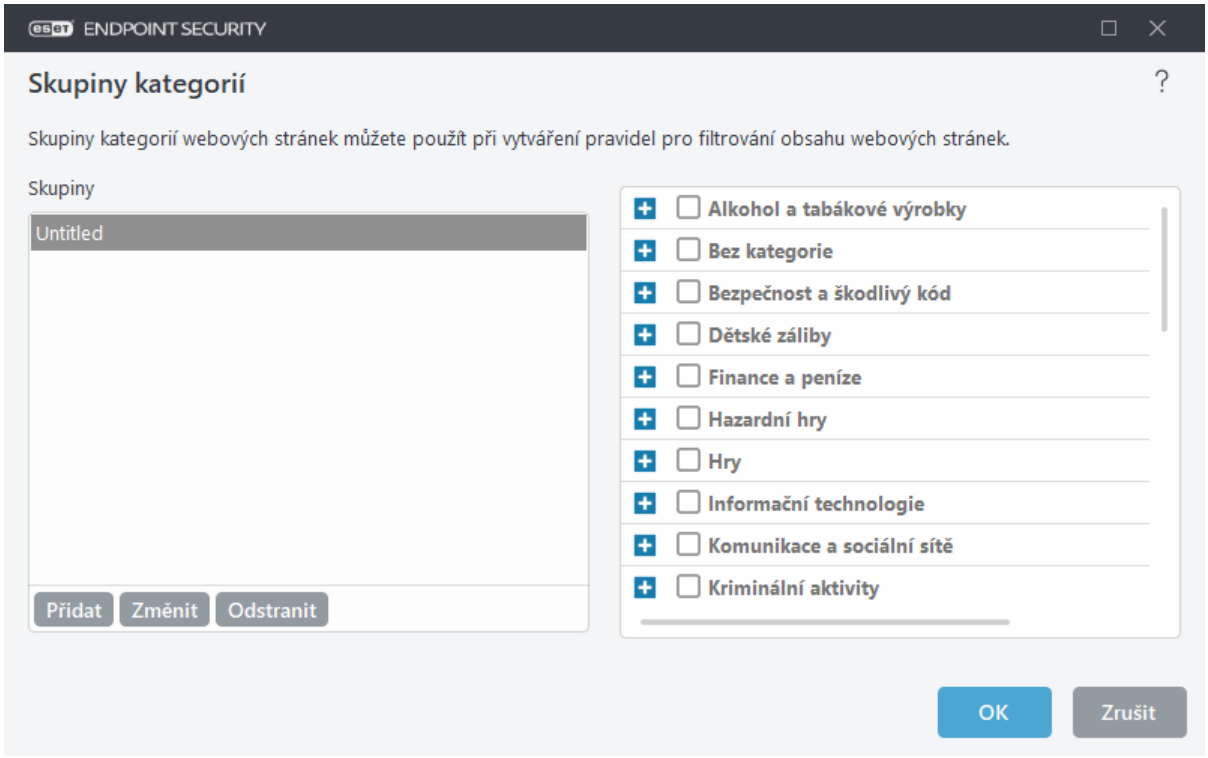
Editor kategorií

Okno editoru kategorií je rozděleno na dvě části. V levé části se nachází seznam existujících skupin kategorií.

- **Přidat** – kliknutím vytvoříte novou skupinu kategorií.
- **Změnit** – kliknutím upravíte existující skupinu kategorií.
- **Odstranit** – vyberte skupinu kategorií, kterou chcete odstranit a klikněte na toto tlačítko.

Pravá část okna obsahuje seznam kategorii a podkategorii. Po kliknutí na kategorii se zobrazí její podkategorie. Každá kategorie obsahuje podkategorie s obsahem pro dospělé a nevhodným obsahem, stejně jako nezávadný obsah. Po otevření editoru a vybrání první skupiny můžete přidat nebo odebrat kategorie/podkategorie ze seznamu odpovídajících skupiny (například násilí a zbraně). Webové stránky s nevhodným obsahem mohou být blokovány a uživatelé mohou být informováni o přístupu na blokovanou webovou stránku.

Pro přidání nebo odebrání kategorie do/ze skupiny použijte zaškrtávací pole.



Níže jsou uvedeny příklady kategorií, jejichž obsah nemusí být na první pohled zřejmý.

- **Různé** – obvykle lokální adresy intranetu, 127.0.0.0/8, 192.168.0.0/16, atd. Pokud stránka vrací chybu 403 nebo 404, pak také patří do této kategorie.
- **Nerozhodnuto** – tato kategorie obsahuje stránky, o kterých nelze rozhodnout z důvodu připojení do databáze rodičovské kontroly.
- **Nezařazeno** – neznámé stránky nezařazené do databáze rodičovské kontroly.
- **Proxy servery** – anonymizéry, přesměrovače nebo veřejné proxy servery používané pro přístup k webovým stránkám, které jsou obvykle Rodičovskou kontrolou zakázány.
- **Sdílení souborů** – stránky, které obsahují velké množství dat například fotografie, videa nebo e-knihy. Takové stránky mohou potenciálně obsahovat škodlivý či nevhodný obsah.

Můžete nahlásit nesprávnou klasifikaci URL adresy.

Podkategorie může patřit pouze do jakékoli skupiny. Některé podkategorie nejsou součástí předdefinovaných skupin (například Hry). Pokud chcete zajistit filtrování určitě kategorie stránek, je nutné ji přidat do konkrétní skupiny.

Editor skupiny URL

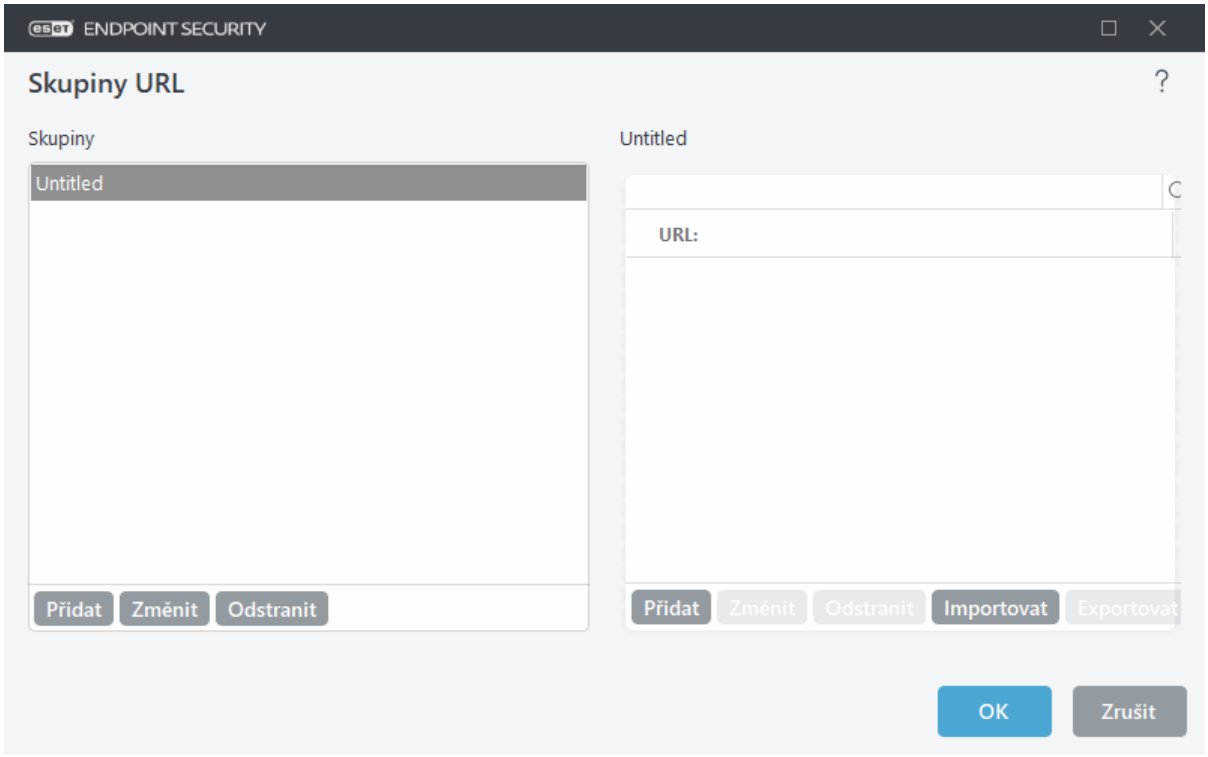
Pomocí editoru skupin URL můžete vytvořit a spravovat skupiny mnoha URL adres, pro které chcete definovat pravidlo (povolují nebo zakazující).

Vytvoření nové skupiny URL

Pro vytvoření nové skupiny URL klikněte na tlačítko **Přidat** a zadejte její název.

Skupiny URL využijete v případě, kdy potřebujete vytvořit pravidlo pro více webových stránek (povolit nebo na ně zablokovat přístup).

Přidání adresy do skupiny URL – ručně



Pro přidání nové adresy do seznamu URL klikněte na tlačítko **Přidat** v pravé části dialogového okna.

V seznamech URL adres není možné používat zástupné znaky * (hvězdička) a ? (otazník).

Není potřeba zadávat celý název domény včetně http:// nebo https://.

Pokud vložíte adresu domény do seznamu, veškerý obsah nacházející se na této doméně a všechny její subdomény (například *sub.examplepage.com*) budou blokovány nebo povoleny na základě definované akce.

V případě konfliktu dvou pravidel ve smyslu, kdy jedno pravidlo přístup na doménu blokuje a druhé povoluje, bude konkrétní doména nebo IP adresa blokována. Pro více informací o vytváření pravidel najdete v části Akce na základě URL.

Přidání adresy do skupiny URL – importováním souboru .txt

Pro importování seznamu URL adres například z .txt souboru (kdy je každá hodnota na novém řádku a soubor je v UTF-8 kódování) klikněte na tlačítko **Importovat**. V seznamech URL adres není možné používat zástupné znaky * (hvězdička) a ? (otazník).

Použití skupin URL v modulu Filtrování obsahu webu

Pro nastavení akci nad konkrétní skupinou URL si otevřete editor pravidel Filtrování obsahu webu, z rozbalovacího menu vyberte požadovanou skupinu URL, přizpůsobte si parametry pravidla a uložte jej kliknutím na tlačítko **OK**.

> Blokování nebo povolení specifické internetové stránky může být přesnější než blokování nebo povolení celé kategorie internetových stránek. Při změně těchto nastavení buďte opatrní.

Přizpůsobení zprávy při přístupu na blokovanou webovou stránku

Pomocí možnosti **Zpráva na zablokované webové stránce** a **Obrázek na zablokované webové stránce** můžete upravit podobu zprávy, která se zobrazí uživateli při přístupu na blokovanou stránku.

Použití

Chystáme se zablokovat kategorii webových stránek "Zbraně".

Příklad zprávy na blokované webové stránce:

```
Přístup na webovou stránku %URL_OR_CATEGORY% byl zablokován, protože se na ní nachá
zí nevhodný nebo škodlivý obsah.
Pro více informací kontaktujte svého administrátora.
```

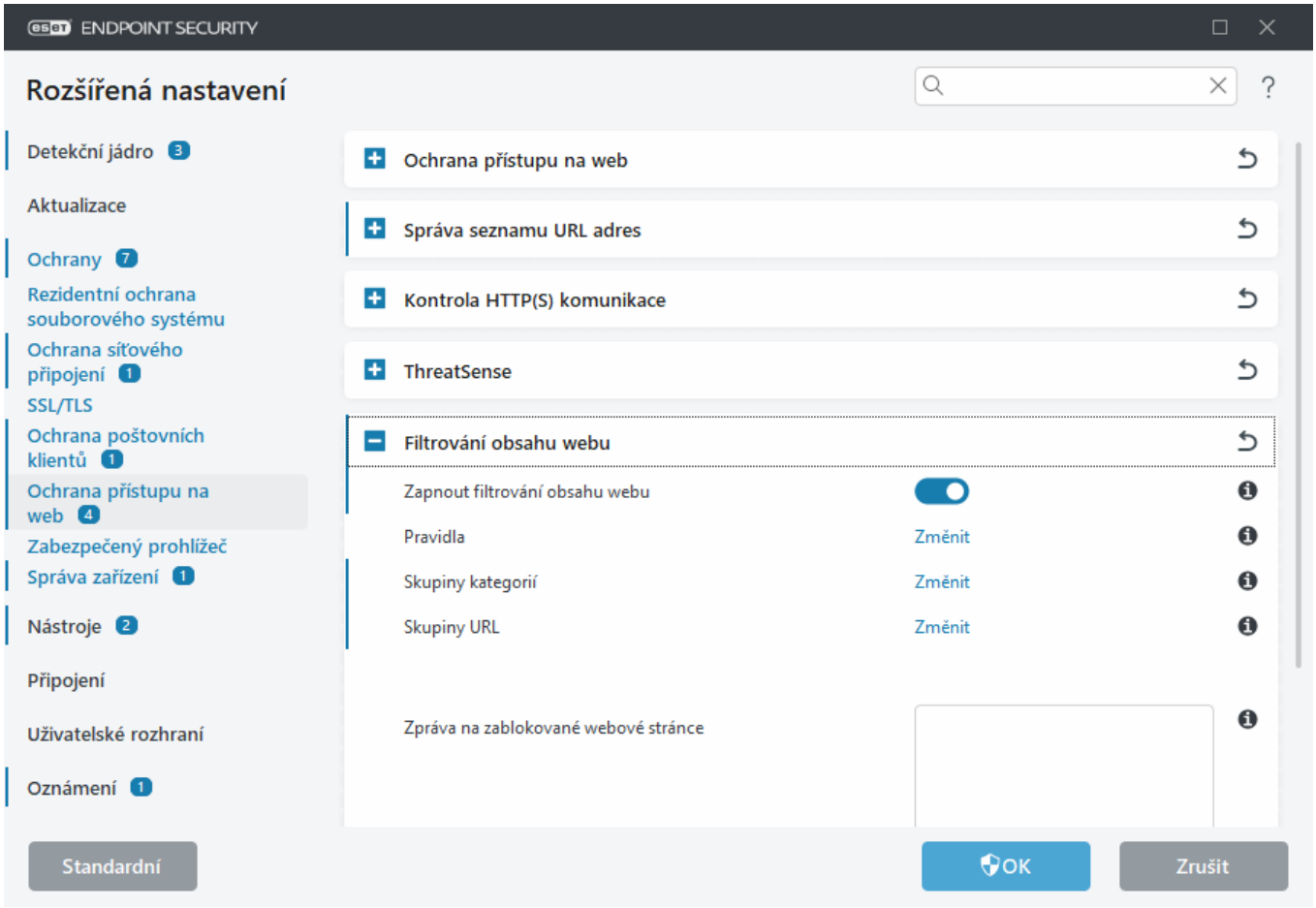
Proměnná	Popis
%CATEGORY%	Kategorie, do níž webová stránka spadá.
%URL_OR_CATEGORY%	Zablokovaná webová stránka nebo kategorie, do níž webová stránka spadá (v závislosti na blokovacím pravidle)
%STR_GOBACK%	Text na tlačítku "Vrátit se zpět"
%product_name%	Název produktu ESET (například ESET Endpoint Security)
%product_version%	Verze produktu ESET

Příklad grafiky na blokované webové stránce:

```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

Pokud je obrázek příliš velký, jeho měřítko se automaticky přizpůsobí (změní se šířka/výška).

Níže je ukázka možné konfigurace v produktu ESET Endpoint Security:



Dialogové okno – Filtrování obsahu webu

Filtrování obsahu webu umožňuje omezit přístup na konkrétní webové stránky všem uživatelům ve firemní síti. Administrátor může definovat kategorie webových stránek, na které chce uživateli nebo skupině uživatelů povolit přístup. Pro konfiguraci této funkce je možné využít skupiny z Active Directory. Tato funkce je standardně vypnuta. Aktivujete ji pomocí přepínače **Zapnout filtrování obsahu webu**. Kliknutím na tlačítko **Změnit** získáte přístup k Editoru pravidel. Předdefinované skupiny webových stránek můžete spravovat po kliknutí na **Změnit** v řádku editoru Skupiny kategorií nebo můžete definovat vlastní adresy pomocí editoru Skupiny URL.

Zabezpečený prohlížeč

Zabezpečený prohlížeč představuje další vrstvu ochrany, která má chránit vaše finanční údaje během online transakcí.

Pro zajištění správného fungování Zabezpečeného prohlížeče musí být zapnutý Reputační systém ESET LiveGrid® (ve výchozím nastavení zapnutý).

Chcete-li konfigurovat chování Zabezpečeného prohlížeče, otevřete Rozšířená nastavení > **Ochrany** > **Zabezpečený prohlížeč**.

K dispozici máte níže uvedené možnosti, jak se má Zabezpečený prohlížeč chovat:

- **Zabezpečení všech prohlížečů** – ve výchozím stavu zapnuto; všechny podporované prohlížeče se budou spouštět v zabezpečeném režimu. Díky tomu můžete prohlížet webové stránky, používat internetové

bankovnictví a provádět online transakce v jednom zabezpečeném okně prohlížeče bez vynuceného přesměrování konkrétních stránek.

- **Přesměrování webových stránek** – webové stránky uvedené na seznamu chráněných stránek a interním seznamu bankovních institucí budou automaticky otevřeny v zabezpečeném prohlížeči. Pro jednotlivé stránky se však můžete rozhodnout, v jakém z prohlížečů (standardním nebo zabezpečeném) se daná stránka otevře.

Přesměrování webových stránek není k dispozici pro zařízení s procesory ARM.

Obecné

Povolit zabezpečený prohlížeč – po aktivování se začne uplatňovat seznam chráněných webových stránek, který budete následně schopni modifikovat.

Ochrana prohlížeče

Zabezpečit všechny prohlížeče – ve výchozím stavu zapnuto; pakliže je tato možnost zapnutá, budou se všechny podporované webové prohlížeče spouštět v zabezpečeném režimu. Díky tomu můžete prohlížet webové stránky, používat internetové bankovnictví a provádět online transakce v jednom zabezpečeném prohlížeči bez vynuceného přesměrování konkrétních stránek.

Režim instalace rozšíření – z rozbalovacího menu vyberte typ rozšíření, jehož instalaci chcete povolit v prohlížečích zabezpečených produktem ESET. Změna nastavení režimu instalace rozšíření nemá vliv na již nainstalovaná rozšíření prohlížeče:

- **Základní rozšíření** – povolena budou pouze ta nejdůležitější rozšíření vyvinutá konkrétním výrobcem prohlížeče.
- **Všechna rozšíření** – dojde k povolení veškerých rozšíření podporovaných konkrétním prohlížečem.

Přesměrování webových stránek

Povolit přesměrování chráněných webových stránek – pokud aktivujete tuto možnost, webové stránky uvedené na seznamu chráněných stránek a interním seznamu bankovních institucí budou automaticky otevřeny v zabezpečeném prohlížeči.

Chráněné webové stránky – pomocí tohoto seznamu definujte, v jakém internetovém prohlížeči (normálním nebo zabezpečeném) se jednotlivé webové stránky otevřou. Ve výchozím nastavení se zobrazí informativní oznámení v prohlížeči a zelený rámeček kolem prohlížeče, který informuje o tom, že je aktivní zabezpečené prohlížení.

Zabezpečit používání online bankovnictví a platebních bran – tato možnost je standardně vypnutá. Po jejím aktivování se kromě URL uvedených na seznamu v sekci Chráněné webové stránky budou v internetovém prohlížeči zabezpečeném produktem ESET automaticky otevírat také webové stránky uvedené na interním seznamu společnosti ESET. Tento seznam spravuje a pravidelně aktualizuje společnost ESET.

Zabezpečený prohlížeč

Rozšířená ochrana paměti – po aktivování této možnosti bude paměť zabezpečeného prohlížeče chráněna před inspekcí jinými procesy.

Ochrana klávesnice – po aktivování této možnosti budou veškeré informace zadané na klávesnici do zabezpečeného prohlížeče skryty před dalšími aplikacemi. Zlepšujeme tak ochranu před keyloggery.

Zelený rámeček prohlížeče – po vypnutí této možnosti se oznámení v prohlížeči a zelený rámeček okolo okna prohlížeče zobrazí pouze při spouštění prohlížeče a poté zmizí.

Nastavit interaktivní upozornění zabezpečeného prohlížeče – umožňuje zobrazit dialogové okno Interaktivních upozornění.

> V některých případech se konkrétní interaktivní upozornění zobrazí pouze v případě výskytu chyby při spouštění Zabezpečeného prohlížeče. Další informace naleznete v kapitole Interaktivní upozornění.

Chráněné webové stránky

ESET Endpoint Security obsahuje vestavěný předdefinovaný seznam známých stránek internetového bankovnictví, které automaticky otevírá v zabezpečeném prohlížeči. Tento seznam můžete kdykoli rozšířit o internetový portál své banky.

Seznam **Chráněných webových stránek** si můžete zobrazit a upravit v Rozšířených nastaveních > **Ochrany** > **Zabezpečený prohlížeč** > **Zabezpečený prohlížeč** > **Chráněné webové stránky** > **Změnit**.

Pravidla v seznamu Chráněné webové stránky určují, zda se má konkrétní webová stránka otevřít v zabezpečeném nebo běžném prohlížeči. Další možnosti nastavení naleznete během **přidání URL**, jak popisujeme níže.

Ovládací prvky

Přidat – kliknutím přidáte do seznamu adresu webové stránky.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odstraníte vybraný záznam.

Importovat/Exportovat – umožňuje exportovat chráněné webové stránky nebo stránky importovat do nového zařízení.

Přidat URL

Webová stránka – HTTPS webová stránka, pro kterou se pravidlo použije.

Otevřít tuto stránku v – zvolte typ prohlížeče, který se má použít při návštěvě této webové stránky:

- **Zabezpečený prohlížeč** – webové stránky jsou přesměrovány do zabezpečeného prohlížeče a jsou chráněny.
- **Běžný prohlížeč** – webové stránky se otevřou v běžném prohlížeči bez dalšího zabezpečení.

Oznámení v prohlížeči

Zabezpečený prohlížeč vás o své stavu informujte prostřednictvím oznámení zobrazovaných v prohlížeči a barevným rámečkem kolem jeho okna.

Oznámení v prohlížeči se zobrazuje v záložce na pravé straně okna prohlížeče.

Oznámení v prohlížeči si rozbalíte kliknutím na ikonu ESET. Kliknutím na oznámení jej minimalizujete. Chcete-li oznámení a zelený rámeček prohlížeče skrýt, klikněte na ikonu (zavřít).

Zrušit lze pouze informativní oznámení a zelený rámeček prohlížeče.

Oznámení v prohlížeči

Typ oznámení	Stav
Informativní oznámení a zelený rámeček prohlížeče	Je zajištěna maximální ochrana a oznámení v prohlížeči je ve výchozím nastavení minimalizované.
Upozornění a oranžový rámeček prohlížeče	Zabezpečený prohlížeč vyžaduje vaši pozornost pro nekritické problémy. Pro zobrazení souvisejících informací nebo řešení postupujte podle kroků uvedených v oznámení v prohlížeči.
Bezpečnostní upozornění a červený rámeček prohlížeče	Prohlížeč není chráněn. Pro zajištění ochrany restartujte prohlížeč. Pro kontrolu konfliktů se soubory načtenými v prohlížeči si otevřete Protokoly > **Zabezpečený prohlížeč** a zajistěte, aby při dalším spuštění prohlížeče nebyly zaznamenané soubory načtené. Pokud problémy přetrvávají, pro vyřešení konfliktu se soubory načtenými prohlížečem kontaktujte technickou podporu společnosti ESET podle pokynů uvedených v naší Databázi znalostí.

Správa zařízení

ESET Endpoint Security automaticky kontroluje zařízení (CD/DVD/USB/atd). Můžete blokovat nebo upravovat rozšířené filtry nebo oprávnění a umožnit uživateli přístup k danému zařízení a práci s ním. Tuto funkci můžete použít v případě, že chcete uživatelům zabránit v připojování výměnných médií k počítači.

Podporovaná externí zařízení:

- Datové úložiště (HDD, USB výměnné jednotky),
- CD/DVD,
- USB tiskárna,
- FireWire úložiště,
- Zařízení Bluetooth,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port,
- Přenosná zařízení (zařízení napájená baterií, jako jsou přehrávače médií, chytré telefony, zařízení plug-and-play, atd.)
- Všechny typy zařízení.

Nastavení správy zařízení můžete upravit v Rozšířeném nastavení > **Ochrany** > **Správa zařízení**.

Přepínačem aktivujte **Povolit ovládání zařízení**, a povolte tak funkci Správa zařízení v ESET Endpoint Security. Aby se tato změna projevila, musíte restartovat počítač. Po zapnutí správy zařízení se zpřístupní odkaz **Pravidla**, prostřednictvím kterého si otevřete editor pravidel.

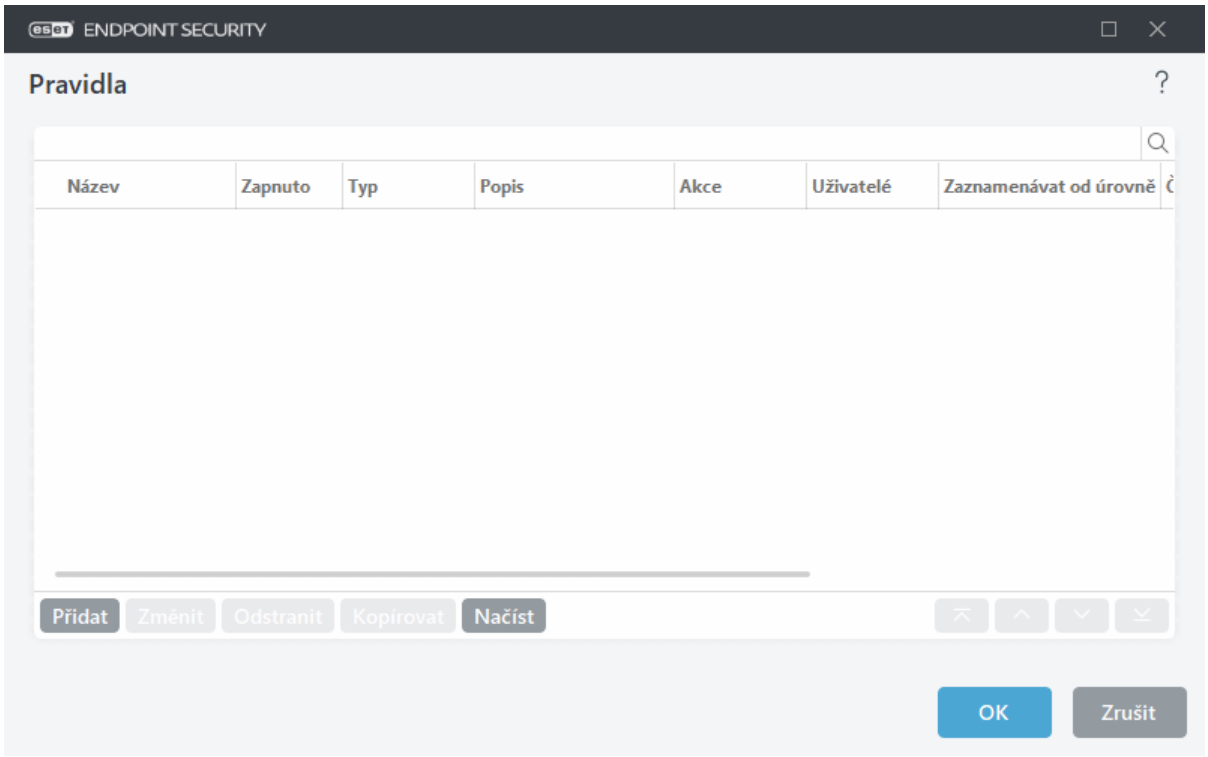
> Skupinu spravovaných zařízení s pravidly můžete importovat ze souboru xml pomocí plánovače. Více informací a průvodce krok za krokem naleznete v ESET Databázi znalostí.

Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování, zobrazí se informační okno a přístup k zařízení bude odepřen.

Editor pravidel ve správě zařízení

Editor pravidel správy zařízení zobrazuje seznam všech existujících pravidel, které umožňují detailní kontrolu nad zařízeními připojovanými k počítači. Více si přečtěte v kapitole Pravidla správy zařízení.

> Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
> Vytvoření a úprava pravidla Správy zařízení v produktu ESET Endpoint (anglicky)



Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování.

Pro správu pravidel klikněte na tlačítko **Přidat** nebo **Změnit**. Pravidlo můžete vymazat kliknutím na tlačítko **Odstranit** nebo pouze deaktivovat pomocí zaškrtávacího pole ve sloupci Zapnuto. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Kopírovat – vytvoří nové pravidlo z již existujícího pravidla.

Kliknutím na tlačítko **Načíst** se automaticky načtou parametry všech připojených výměnných zařízení připojených k počítači.

Pravidla jsou seřazena dle priority, tedy pravidlo s nejvyšší prioritou je umístěno nahoře. Pořadí pravidel můžete upravit pomocí tlačítek **Nahoru/Výše/Dolů/Níže**.

Do protokolu správy zařízení se zapíšou informace o všech připojených zařízeních. Protokoly z fungování tohoto modulu naleznete v hlavním okně programu ESET Endpoint Security na záložce **Nástroje** > **Protokoly**.

Detekovaná zařízení

Kliknutím na tlačítko **Načíst** se zobrazí informace o všech aktuálně připojených zařízeních, jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné).

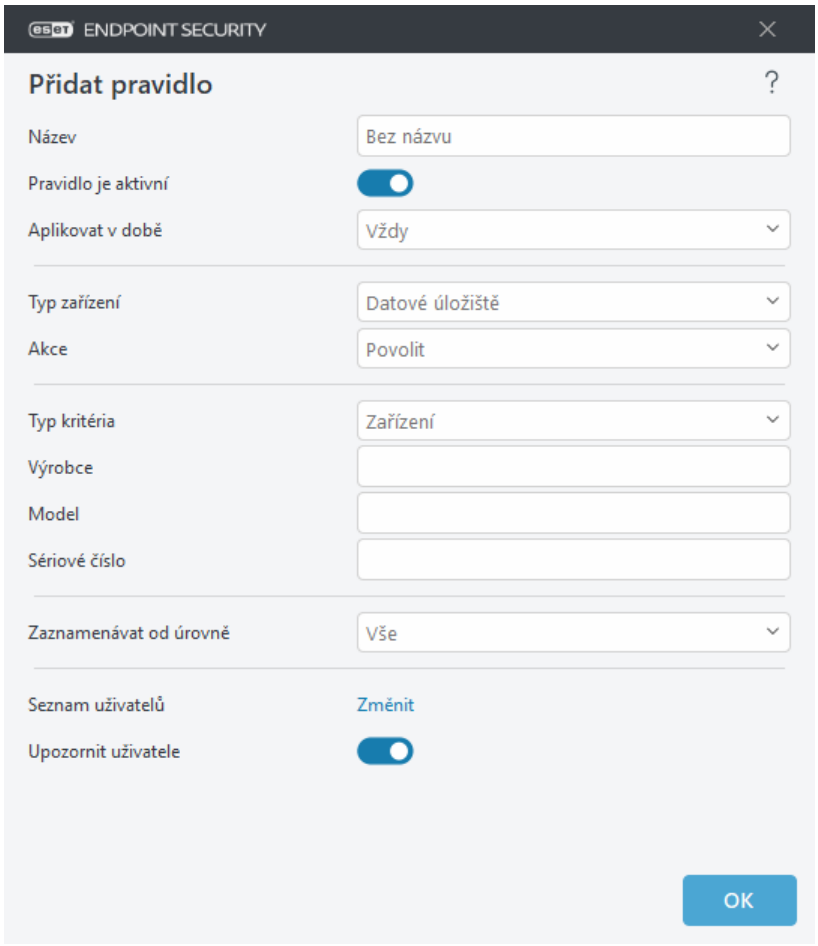
Po vybrání konkrétního zařízení a kliknutí na tlačítko **OK** se zobrazí dialogové okno pro vytvoření nového pravidla s již předdefinovanými hodnotami (zobrazené hodnoty můžete dle potřeby upravit).

Zařízení v režimu nízké spotřeby (režim spánku) jsou označena vykřičníkem . V takovém případě pro zaktivnění tlačítka **OK**, a dokončení vytvoření pravidla pro dané zařízení, proveďte následující kroky:

- Odpojte a znovu připojte zařízení.
- Použijte zařízení (například spusťte aplikaci Kamera ve Windows a probuďte webovou kameru).

Vytvoření nového pravidla

V tomto okně můžete definovat akce, které se provedou po připojení daného zařízení k počítači.



Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla. Kliknutím na přepínač vedle **Pravidlo je aktivní** dané pravidlo zakážete nebo povolíte; to může být užitečné, pokud nechcete pravidlo trvale odstranit.

Aplikovat v době – prostřednictvím časových slotů může být pravidlo aktivní pouze v definované době. Nejprve sloty vytvořte, poté je můžete vybrat v tomto rozbalovacím menu. Více informací si přečtěte v kapitole Časové sloty.

Typ zařízení

Z rozbalovacího menu vyberte typ zařízení (diskové úložiště/přenosné zařízení/Bluetooth/FireWire/…). Typy zařízení se přebírají ze systému a můžete si je zobrazit v systémovém Správci zařízení, který poskytuje informace o zařízeních připojených k počítači. Úložná média zahrnuje externí disky nebo čtečky paměťových karet připojených pomocí USB nebo FireWire. Čtečky čipových karet zahrnují čtečky karet s integrovanými elektronickými obvody jako jsou SIM karty nebo přístupové karty. Příkladem zobrazovacích zařízení jsou fotoaparáty a kamery, které neposkytují informace o uživateli, pouze vyvolávají akce. To znamená, že tato zařízení mohou být blokována pouze globálně.

> Seznam uživatelů není dostupný pro modemy. Pravidlo týkající se modemu bude platné pro všechny uživatele.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

- **Povolit** – plný přístup k zařízení,
- **Blokovat** – přístup k zařízení bude zakázán,
- **Blokovat zápis** – uživatel může pouze číst soubory na daném zařízení, ale ne zapisovat.
- **Upozornit** – při každém připojení zařízení se uživateli zobrazí upozornění, že byl přístup na zařízení povolen/zakázán a zároveň se informace zapíše do protokolu. K zapamatování zařízení nedochází. Při opětovném připojení stejného zařízení dojde k zobrazení oznámení.

Mějte na paměti, že uvedené akce nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

Typ kritéria

Vyberte, zda chcete pravidlo vytvořit pro jednotlivé **zařízení** nebo **skupinu zařízení.**

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.

Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.

Tip: Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a podívejte se do protokolu správy zařízení.

Zaznamenávat do protokolu

- **Vše** – zaznamenají se všechny události.
- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů,
- **Informační** – zaznamenány budou informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – obsahují varovné zprávy a kritické chyby. Zároveň se při této úrovni budou události zasílat také na ERA Server.
- **Žádné** – nebudou zaznamenávány žádné události, nevytvoří se žádné protokoly.

Pravidla můžete přiřadit konkrétnímu uživateli nebo celé skupině uživatelů pomocí dialogového okna **Seznam uživatelů**:

- **Přidat** – otevře okno **Vybrat typ objektu: Uživatelé nebo Skupiny**, kde můžete vybrat konkrétní uživatele.
- **Odstranit** – odebere vybraného uživatele z filtru.

Omezení v seznamu uživatelů

Seznam uživatelů není možné definovat v pravidlech platných pro níže uvedené Typy zařízení:

- USB tiskárna,
- Bluetooth zařízení,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port.

Upozornit uživatele – Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování a zobrazí se okno s oznámením.

Skupiny zařízení

Zařízení připojená k počítači mohou představovat bezpečnostní riziko.

Dialogové okno skupin zařízení je rozděleno na dvě části. V levé části se nachází seznam vytvořených skupin a v pravé části se zobrazují zařízení, která patří do dané skupiny. Pokud si chcete zobrazit v pravém okně zařízení, vyberte vlevo konkrétní skupinu zařízení.

Jakmile máte vybranou konkrétní skupinu, po kliknutí na příslušné tlačítko můžete zařízení do skupiny přidat nebo odstranit. Další možností přidání je import zařízení ze souboru. V neposlední řadě si kliknutím na tlačítko **Načíst** můžete zobrazit seznam všech zařízení připojených k počítači. Následně se vám zobrazí dialogové okno **Detekovaná zařízení**. Vyberte zařízení ze seznamu a přidejte je do skupiny kliknutím na tlačítko **OK**.

Ovládací prvky

Přidat – vytvoří novou skupinu nebo přidá zařízení do již existující skupiny, s ohledem na to, zda jste klikli na stejnojmenné tlačítko v levé nebo pravé části okna.

Změnit – můžete upravit název vybrané skupiny nebo parametry zařízení (výrobce, model, sériové číslo).

Odstranit – vymaže vybranou skupinu nebo konkrétní zařízení.

Importovat – pomocí této možnosti importujte seznam zařízení z textového souboru. Soubor musí splňovat následující formát:

- Každé zařízení je uvedeno na samostatné řádku.
- **Výrobce**, **Model** a **Sériové číslo** pro každé zařízení musí být odděleno čárkou.

Příklad obsahu textového souboru:
```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Exportovat – pomocí této možnosti exportujete seznam zařízení do souboru.

Kliknutím na tlačítko **Načíst** se zobrazí informace o všech aktuálně připojených zařízeních, jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné).

Skupinu spravovaných zařízení s pravidly můžete importovat ze souboru xml pomocí plánovače. Více informací a průvodce krok za krokem naleznete v ESET Databázi znalostí.

Přidat zařízení

Kliknutím na tlačítko Přidat přidáte nové zařízení do existujícího seznamu zařízení. Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.
- **Popis** – váš vlastní popis zařízení pro zjednodušení orientace v seznamu.

Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.

Kliknutím na tlačítko **OK** uložíte změny. Klikněte na tlačítko **Zrušit** pro zavření dialogového okna bez uložení změn.

Po vytvoření skupiny zařízení je třeba pro ni přidat nové pravidlo a zvolit akci, která se má provést.

Mějte na paměti, že uvedené akce nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v Rozšířeném nastavení pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochran kromě Kontroly počítače.

Kontrolované objekty

V této sekci můžete vybrat součásti počítače a soubory, které budou testovány na přítomnost infiltrace.

Operační paměť – kontrola přítomnosti hrozeb, které mohou být zavedeny v operační paměti počítače.

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do slovníku pojmů.

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

Archivy – podporovány jsou formáty ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE (Outlook Express) a soubory.

Samorozbalovací archivy – archivy které nepotřebují pro své rozbalení jiné programy. Jedná se o SFX (Self-extracting) archivy.

Runtime archivy – runtime archivy se na rozdíl od klasických archivů po spuštění rozbalí v paměti počítače. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG aj.) program podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

Rozšířená heuristika/DNA/Smart vzorky – rozšířená heuristika se skládá z unikátních heuristických algoritmů vyvinutých společností ESET optimalizovaných pro detekci počítačových červů a trojských koňů napsaných ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopni produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých škodlivých kódů.

Léčení

Nastavení léčení ovlivňuje chování ESET Endpoint Security během léčení objektů.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci detekčního jádra ThreatSense pro volitelnou kontrolu počítače jsou v části **Ostatní** k dispozici také následující možnosti:

Kontrolovat alternativní datové proudy (ADS) – alternativní datové proudy používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho infiltrací je proto využívá jako maskování před případným odhalením.

Spustit kontrolu na pozadí s nízkou prioritou – každá kontrola počítače využívá určité množství systémových zdrojů. Pokud právě pracujete s programy náročnými na výkon procesoru, přesunutím kontroly na pozadí jí můžete přiřadit nižší prioritu a získat více prostředků pro ostatní aplikace.

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do protokolu zapíší všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnuté Smart optimalizaci je použito nejoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena. V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány. Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik). Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: 3 GB.

Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Úrovně léčení

Chcete-li změnit nastavení úrovně léčení pro určitý ochranný modul, rozbalte položku **ThreatSense** (například **Rezidentní ochrana souborového systému**) a poté z rozbalovacího menu vyberte **Úroveň léčení**.

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET Endpoint Security

Úroveň léčení	Popis
Vždy vyřešit infekci	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých ojedinělých případech vyléčit (např. u systémových souborů), bude detekovaný objekt ponechán v původním umístění. Jedná se o **doporučené výchozí nastavení** ve spravovaných prostředích.

Úroveň léčení	Popis
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučené pro většinu případů.
Vždy se dotázat uživatele	V průběhu léčení objektů se uživateli zobrazí interaktivní okno, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Tato úroveň je určená zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Přípony souborů vyloučených z kontroly

Přípony vyloučených souborů jsou součástí ThreatSense. Chcete-li nakonfigurovat přípony vyloučených souborů, klikněte na **ThreatSense** v Rozšířeném nastavení pro jakýkoli modul, který používá technologii ThreatSense.

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

> Nezaměňujte tuto funkci s možností pro vyloučení procesů, tvorbu HIPS výjimek nebo vyloučení souborů/složek.

Standardně jsou kontrolovány všechny soubory. Do seznamu souborů vyloučených z kontroly můžete přidávat libovolné přípony.

Definovat výjimky je někdy nezbytné, jestliže jsou kontrolovány soubory s určitým rozšířením a kontrola by mohla mít negativní vliv na běh programu. Může být vhodné vyloučit např. `.edb`, `.eml` a `.tmp` pro MS Exchange Server).

> Pro přidání přípony klikněte na tlačítko **Přidat**. Do zobrazeného prázdného pole zadejte příponu (například tmp) a akci potvrďte kliknutím na tlačítko **OK**. Zadat můžete **více hodnot** oddělené čárkou, středníkem nebo zadejte každou příponu na nový řádek (například po vybrání možnosti **Středník** můžete zadat `edb;eml;tmp`).
> Při definování seznamu výjimek můžete použít jako zástupný znak ? (otazník). Otazník reprezentuje jeden znak (například `?db`).

> Chcete-li v operačním systému Windows zobrazit příponu souboru (pokud existuje), musíte zaškrtnout políčko **Přípony názvů souborů** v **Průzkumníku Windows** > **Zobrazit**.

Doplňující parametry skenovacího jádra ThreatSense

Chcete-li upravit tato nastavení, otevřete Rozšířená nastavení > **Ochrany** > **Rezidentní ochrana souborového systému** > **Další parametry ThreatSense**.

Doplňující parametry ThreatSense pro nově vytvořený nebo upravený soubor

Pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s doplňujícími parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána rozšířená heuristika ESET Endpoint Security, čímž se výrazně zvyšuje úroveň detekce, i když škodlivý kód ještě není znám před vydáním aktualizace detekčního jádra.

Kromě nově vytvářených souborů se kontrolují také **Samorozbalovací soubory** (.sfx) a **Runtime packery** (interně komprimované spustitelné soubory). Standardně jsou archivy kontrolovány do 10 úrovně vnoření bez ohledu na jejich velikost. Pro změnu nastavení kontroly archivů deaktivujte pomocí přepínače možnost **Standardní nastavení kontroly archivů**.

Doplňující parametry ThreatSense pro spouštěné soubory

Rozšířená heuristika pro spouštěné soubory – rozšířená heuristika se pro spouštěné soubory používá standardně. Pokud je zapnutá, důrazně doporučujeme ponechat zapnutou také Smart optimalizaci a ESET LiveGrid® pro snížení dopadu na výkon systému.

Rozšířená heuristika při spuštění souboru z výměnných médií – rozšířená heuristika emuluje kód aplikace ve virtuálním prostředí a vyhodnotí chování aplikace ještě předtím, než je povoleno aplikaci spuštění z výměnného média.

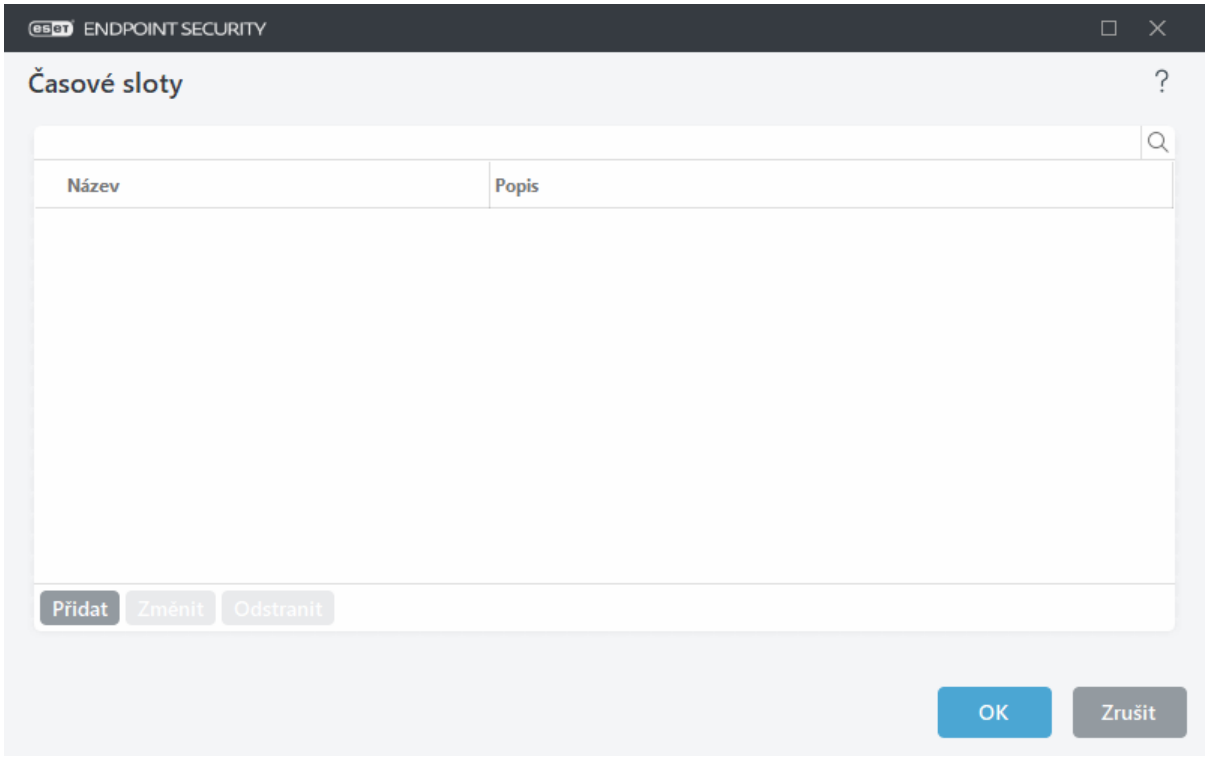
Nástroje

V Rozšířeném nastavení > **Nástroje** můžete nakonfigurovat pokročilá nastavení funkcí, které nabízejí dodatečné zabezpečení a pomáhají zjednodušit správu ESET Endpoint Security.

- Časové sloty
- Aktualizace operačního systému Windows
- ESET CMD
- Vzdálené monitorování a správa (RMM)
- Interval ověření licence
- Protokoly
- Prezentační režim
- Diagnostika

Časové sloty

Časové sloty lze vytvořit a následně přiřadit pravidlům pro **Správu zařízení** a **Filtrování obsahu webu**. Vytvořit si je můžete v **rozšířeném nastavení** v sekci Nástroje > **Časové sloty**. Díky této logice si můžete vytvořit časové sloty pro často používané rozsahy času (pracovní doba, víkend aj.) a následně je více násobně používat při tvorbě pravidel – aniž byste museli čas pokaždé znovu definovat. Časové sloty můžete používat v pravidlech, které podporují správu času.



Pro vytvoření časového slotu:

1. Klikněte v rozšířeném nastavení v sekci Nástroje > Časové sloty na **Změnit** a dále na tlačítko **Přidat**.
2. Zadejte **název**, volitelně popis, časového slotu a klikněte na tlačítko **Přidat**.
3. V zobrazeném dialogovém okně definujte počátek a konec časového slotu, případně použijte přepínač **Celý den**.
4. Akci potvrďte kliknutím na tlačítko **OK**.

V jednom časovém slotu můžete definovat více časových rozsahů. Když je časový interval vytvořen, zobrazí se v rozbalovacím menu **Aplikovat v době** v okně editoru pravidel správy zařízení nebo v okně editoru pravidel pro filtrování obsahu webu.

Aktualizace operačního systému Windows

Aktualizace operačního systému Windows představují důležitou součást pro zajištění ochrany uživatelů před zneužitím bezpečnostních děr a tím pádem možným infikováním systému. Z tohoto důvodu je vhodné instalovat aktualizace Microsoft Windows co nejdříve po jejich vydání. V ESET Endpoint Security můžete nastavit, od jaké úrovně chcete být informováni na chybějících systémové aktualizace. K dispozici jsou následující možnosti:

- **Žádné aktualizace** – nebudou nabízeny žádné aktualizace,
- **Volitelné aktualizace** – budou nabízeny aktualizace s nízkou prioritou a všechny následující,
- **Doporučené aktualizace** – budou nabízeny běžné aktualizace a všechny následující,
- **Důležité aktualizace** – budou nabízeny důležité aktualizace a všechny následující,
- **Kritické aktualizace** – budou nabízeny pouze kritické aktualizace.

Kliknutím na tlačítko **OK** uložíte změny. Zobrazení okna dostupných aktualizací proběhne po ověření stavu na aktualizačním serveru. Samotné zobrazení dostupných aktualizací proto nemusí nutně proběhnout ihned po uložení změn.

Dialogové okno – Aktualizace operačního systému

Pokud jsou pro váš operační systém dostupné aktualizace, ESET Endpoint Security vás na to v hlavním okně programu upozorní. Po kliknutí na možnost **Více informací** se zobrazí dialogové okno s přehledem dostupných aktualizací.

V tomto dialogovém okně naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Řazeny jsou dle názvu a vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Dvojklikem na konkrétní aktualizaci si zobrazíte podrobné informace o dané aktualizaci.

Kliknutím na možnost **Spustit aktualizaci systému** stáhnete a nainstalujte všechny uvedené aktualizace operačního systému.

Informace o aktualizacích

V dialogovém okně Aktualizace systému naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Tlačítkem **Spustit aktualizace systému** zahájíte stahování a instalaci aktualizací operačního systému.

Po kliknutí pravým tlačítkem myši na danou aktualizaci a vybrání možnosti **Zobrazit informace** se zobrazí podrobné informace o aktualizaci.

ESET CMD

Jedná se o funkci, která povolí používání pokročilých ecmd příkazů. Exportovat a importovat nastavení můžete prostřednictvím příkazového řádku (ecmd.exe). Až dosud bylo možné exportovat nastavení pomocí GUI. Export konfigurace ESET Endpoint Security můžete provést do souboru formátu *.xml*.

Po zapnutí funkce ESET CMD (v **Rozšířeném nastavení** v sekci **Nástroje** > **ESET CMD**) pomocí přepínače do polohy zapnuto si vyberte způsob ověření:

- **Žádný** – pokud vyberete tuto možnost, nebude vyžadováno ověření. Toto nedoporučujeme, protože hrozí potenciální bezpečnostní riziko umožněním importu nepodepsaných konfigurací.
- **Heslo pro přístup do rozšířeného nastavení** – pro ověření se použije heslo, které chrání přístup do nastavení produktu. V tomto případě při importování konfigurace z *.xml* souboru dojde k ověření, zda je soubor podepsán (návod na podepsání naleznete níže) a podpis odpovídá heslu pro přístup do nastavení. Před importováním konfigurace již musí být definováno heslo pro přístup do nastavení. Konfigurace se neimportuje pokud nemáte nastavenu ochranu heslem, heslo nesouhlasí nebo importovaný *.xml* soubor není podepsán.

Poté, co aktivujete funkci ESET CMD, můžete pro importování a exportování konfigurace produktu ESET Endpoint Security používat příkazový řádek. Příkazy můžete pouštět manuálně, případně si operace v rámci automatizace naskriptovat.

Pro použití ecmd příkazů musíte mít oprávnění administrátora, resp. je třeba Příkazový řádek **spustit jako administrátor**. V opačném případě se zobrazí chyba **Error executing command**. Při exportování konfigurace musí cílová složka existovat. Export je možný i v případě, kdy je funkce ESET CMD v produktu vypnutá.

Pokročilé příkazy ecmd lze spustit pouze lokálně. Příkazy na dočasné pozastavení (pause) je možné spouštět pouze vzdáleně pomocí klientské úlohy **Spustit příkaz** z ESET PROTECT.

Konfiguraci z nainstalovaného produktu exportujete příkazem:
`ecmd /getcfg c:\config\settings.xml`
Konfiguraci do nainstalovaného produktu naimportujete příkazem:
`ecmd /setcfg c:\config\settings.xml`

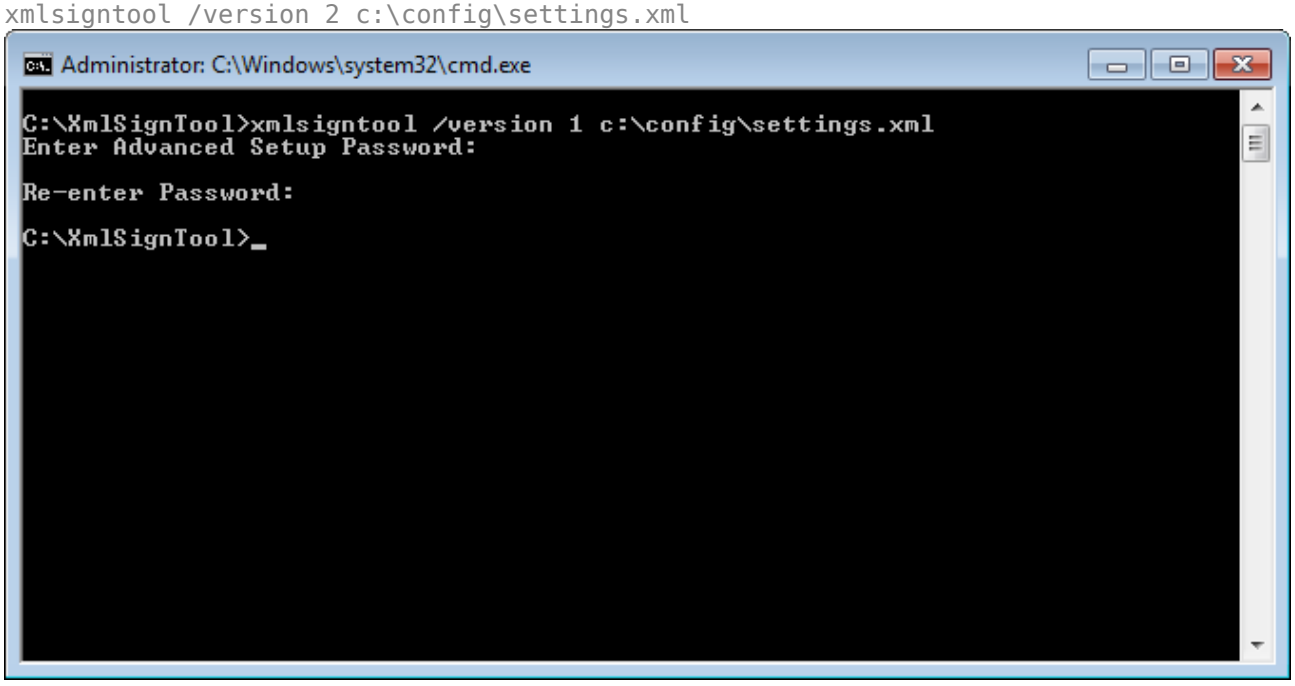
Jak podepsat *.xml* konfigurační soubor:

1. Z webových stránek společnosti ESET si stáhněte nástroj XmlSignTool.
2. Příkazový řádek **Spusťte jako administrátor** (cmd).
3. Přejděte do složky se staženým nástrojem `xmlsigntool.exe`.
4. Konfigurační příkaz *.xml* podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`

Hodnota parametru `/version` závisí na verzi ESET Endpoint Security. Pro verzi 7 a novější použijte `/version 2`.

5. Zadejte heslo, které jste si nastavili pro přístup do nastavení. Následně bude váš *.xml* soubor s konfigurací programu podepsán a můžete jej prostřednictvím ESET CMD importovat do jiné instalace ESET Endpoint Security.

Příkaz pro podepsání konfiguračního souboru:
`xmlsigntool /version 2 c:\config\settings.xml`



V případě, že změníte heslo pro přístup do nastavení a budete chtít prostřednictvím ESET CMD importovat konfiguraci z *.xml* souboru podepsaného původním heslem, podepište jej nejprve aktuálním heslem. Tímto budete moci využít starší konfigurační soubor, aniž byste jej museli před importem exportovat z jiné běžící instalace ESET Endpoint Security.

Aktivováním ESET CMD bez nastaveného ověřování představuje bezpečnostní riziko a nedoporučujeme tuto možnost používat v produkčních prostředích. V takovém případě je možné do produktu importovat nepodepsané konfigurace. Pokud dosud nemáte nastaveno heslo pro ochranu produktu, přejděte v rozšířeném nastavení do sekce **Uživatelské rozhraní** > **Přístup k nastavení**.

Seznam ecmd příkazů

Jednotlivé bezpečnostní funkce je možné zapínat a dočasně vypínat z ESET PROTECT prostřednictvím klientské úlohy Spustit příkaz. Příkazy nemění nastavení vynucené politikou a k opětovnému nastavení dané funkce dojde po zapnutí součásti nebo restartování zařízení. Pro použití ecmd příkazu zadejte jeho přesné znění při vytváření úlohy do pole příkaz ke spuštění.

Zde uvádíme souhrnný přehled dostupných příkazů:

Bezpečnostní funkce	Příkaz pro dočasné pozastavení	Příkaz pro zapnutí
Rezidentní ochrana souborového systému	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Ochrana dokumentů	ecmd /setfeature document pause	ecmd /setfeature document enable
Správa zařízení	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Prezentační režim	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Ochrana proti síťovým útokům (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Ochrana proti zapojení do botnetu	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Filtrování obsahu webu	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Ochrany přístupu na web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Ochrana poštovních klientů	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispamová ochrana poštovních klientů	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-Phishingová ochrana	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Vzdálené monitorování a správa (RMM)

Remote Monitoring and Management (RMM) je způsob pro vzdálené monitorování a ovládání aplikací prostřednictvím lokálně nainstalovaného agenta poskytnutého MSP (Managed Service Provider).

ERMM – ESET plugin pro RMM

- Součástí standardní instalace ESET Endpoint Security je soubor `ermm.exe`, který naleznete ve složce s produktem:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` je nástroj příkazového řádku vyvinutý společností ESET určený ke správě firemních bezpečnostních produktů a komunikaci s libovolným RMM pluginem.
- `ermm.exe` si vyměňuje data s RMM pluginem, který komunikuje s RMM agentem napojeným na RMM server. Ve Výchozí konfiguraci je ESET RMM nástroj deaktivovaný.

Další zdroje

- ERMM příkazový řádek
- Seznam ERMM JSON příkazů
- Jak aktivovat vzdálené monitorování a správu produktu (RMM) v ESET Endpoint Security?

ESET Direct Endpoint Management pluginy pro RMM řešení třetích stran

RMM Server běží jako služba na serveru třetí strany. Pro více informací se podívejte do konkrétních online uživatelských příruček ESET Direct Endpoint Management:

- ESET Direct Endpoint Management Plug-in pro ConnectWise Automate
- ESET Direct Endpoint Management Plugin pro DattoRMM
- ESET Direct Endpoint Management pro Solarwinds N-Central
- ESET Direct Endpoint Management pro NinjaRMM

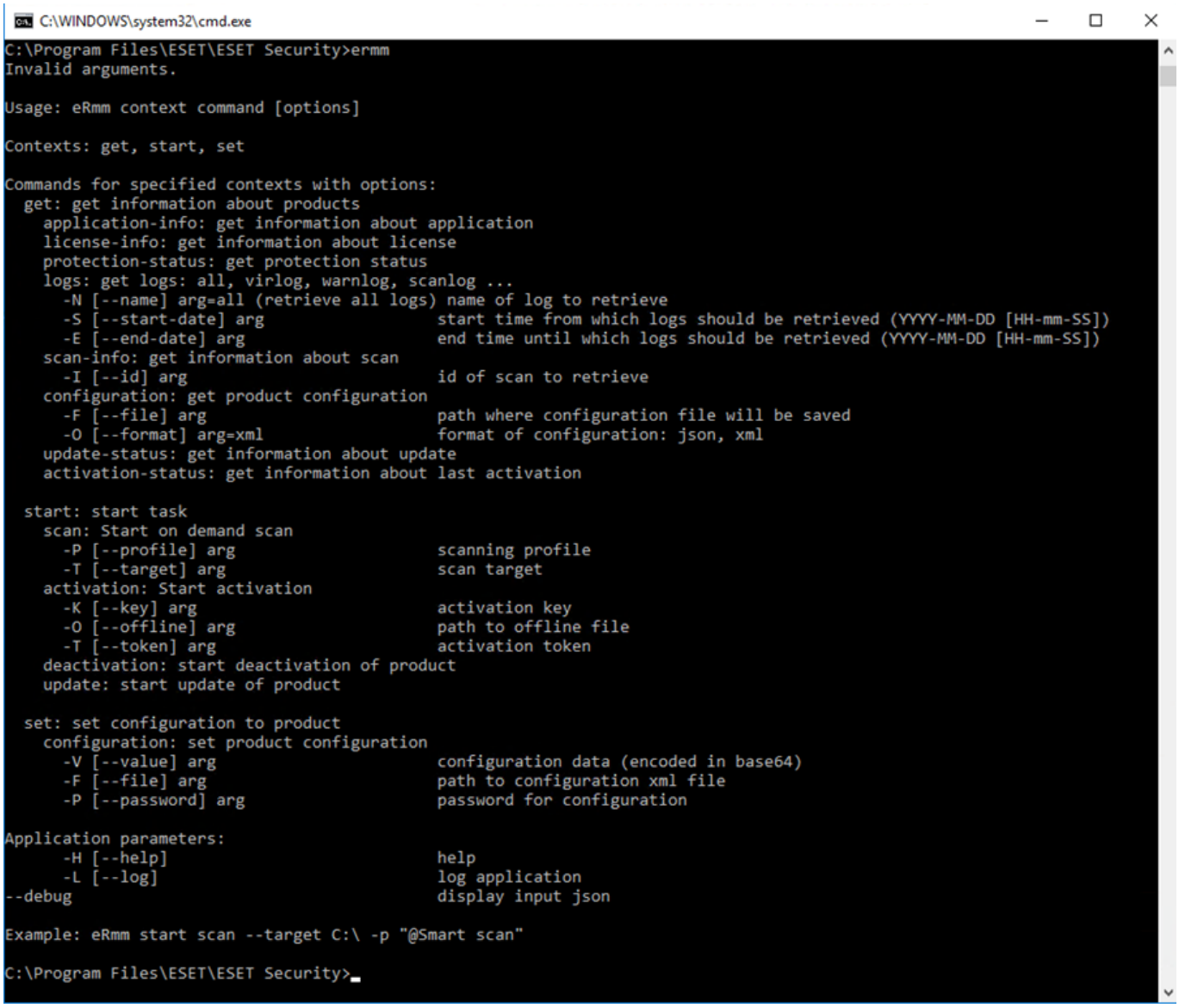
ERMM příkazový řádek

Vzdálené monitorování a správa se spouští pomocí příkazového řádku. Součástí standardní instalace ESET Endpoint Security je soubor ermm.exe, který naleznete ve složce s produktem Endpoint: *C:\Program Files\ESET\ESET Security*.

Spusťte příkazový řádek (cmd.exe) jako správce a přejděte do adresáře (pro otevření příkazového řádku stiskněte klávesy Windows + R, do zobrazeného okna Spustit zadejte cmd a potvrďte klávesou Enter).

Syntaxe příkazu je: `ermm context command [options]`

V parametrech protokolu se rozlišují malá a velká písmena.



ehm.exe používá tři základní kontexty: Get, Start a Set. V následující tabulce naleznete příklady syntaxe příkazů. Po kliknutí na odkaz ve sloupci Příkaz si zobrazíte další možnosti, parametry a příklady použití. Po úspěšném provedení příkazu se zobrazí výsledek s výstupními daty. Pro zobrazení vstupních dat přidejte do příkazu parametr `--debug`.

Kontext	Příkaz	Popis
get		**Získání informací o produktech**
	application-info	Získání informace o produktu
	license-info	Získání informace o licenci
	protection-status	Získání stavu ochrany
	logs	Získání protokolů
	scan-info	Získání informace o spuštění kontroly
	configuration	Získání konfigurace produktu
	update-status	Získání informace o aktualizaci
	activation-status	Získání informace o poslední aktivaci
start		**Start task**
	scan	Spuštění volitelné kontroly

Kontext	Příkaz	Popis
	activation	Spuštění aktivace produktu
	deactivation	Spuštění deaktivace produktu
	update	Spuštění aktualizace produktu
set		**Nastavení možností produktu**
	configuration	Nastavení konfigurace produktu

Ve výsledku každého příkazu je první zobrazenou informací ID výsledku. Chcete-li lépe porozumět informacím o výsledcích, podívejte se do níže uvedené tabulky ID.

ID chyby	Chyba	Popis
0	Success	
1	Command node not present	Uzel příkazu ("command") se nenachází ve vstupních datech formátu JSON
2	Command not supported	Konkrétní příkaz není podporován
3	General error executing the command	Chyba při provádění příkazu
4	Task already running	Požadovaná úloha je již spuštěna a proto nebyla opětovně spuštěna
5	Invalid parameter for command	Chybný uživatelský vstup
6	Command not executed because it's disabled	Funkce Vzdáleného monitorování a správy není v Rozšířených nastaveních aktivována nebo není spuštěna v režimu správce

Seznam ERMM JSON příkazů

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Příkazový řádek

```
ermm.exe get protection-status
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

Příkazový řádek

```
ermm.exe get application-info
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Příkazový řádek

```
ermm.exe get license-info
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Příkazový řádek

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Příklad

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

Příkazový řádek

```
ermm.exe get activation-status
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Získání informace o spuštění kontroly.

Příkazový řádek

```
ermm.exe get scan-info
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Žádná data

Příklad

call

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Příkazový řádek

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Příklad

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Příkazový řádek

```
ermm.exe get update-status
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Příkazový řádek

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Příklad

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Příkazový řádek

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Name	Value
key	Activation key

offline	Path to offline file

Příklad

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Příkazový řádek

```
ermm.exe start deactivation
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Příkazový řádek

```
ermm.exe start update
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

None

Příklad

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Příkazový řádek

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parametry – parametry, s nimiž bude aplikace spuštěna (nepovinné).

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Příklad

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Interval ověření licence

ESET Endpoint Security se automaticky připojuje k licenčním serverům společnosti ESET. Počet připojení k licenčnímu serveru ESET můžete omezit v Rozšířených nastaveních > **Nástroje** > **Licence**. Ve výchozím nastavení je **Interval ověření** nastavena na hodnotu **Automaticky** a připojení je navázáno několikrát za hodinu. V případě potřeby můžete **Interval ověření** změnit na **Omezeně**, a snížit tak množství přenášených dat. Pokud je vybrána možnost **Omezeně**, ESET Endpoint Security se připojuje k licenčnímu serveru pouze jednou denně nebo při restartu počítače.

Pokud nastavíte **Interval ověření** na **Omezeně**, všechny změny související s licencí provedené na portále ESET HUB / ESET MSP Administrator se v nastavení ESET Endpoint Security mohou projevit až po uplynutí jednoho dne.

Protokoly

Konfiguraci protokolování ESET Endpoint Security najdete v Rozšířených nastaveních > **Nástroje** > **Protokoly**. V této sekci můžete upravit způsob správy protokolů. Program dokáže automaticky odstraňovat staré protokoly, čímž šetří místo na disku. V nastavení můžete vybrat následující možnosti:

Zaznamenávat události od úrovně – umožňuje nastavit úroveň, od které se budou zaznamenávat události do protokolu.

- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informační** – jedná se o informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíší kritické chyby, chybová a varovná hlášení.
- **Chyby** – kromě kritických varování se zaznamenají chyby typu "Chyba při stahování souboru aktualizace".

- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany, neúspěšná inicializace firewallu, ...)

> Všechna zablokovaná spojení se do protokolu zapíší při vybrání **diagnostické** úrovně.

Pomocí možnosti **Automaticky vymazat záznamy starší než (dní)** můžete nastavit, po kolika dnech se záznamy mají vymazat.

Automaticky optimalizovat protokoly – pokud aktivujete tuto možnost, protokoly budou automaticky defragmentovány po dosažení mezní hranice definované v polii **Při překročení počtu nevyužitých záznamů (v procentech)**.

Kliknutím na **Optimalizovat** spustíte defragmentaci protokolů. Defragmentace odstraňuje prázdné záznamy v protokolech, čímž zvyšuje rychlost zpracovávání. Viditelné zlepšení práce s protokoly je po optimalizaci znatelné hlavně především u protokolů s velkým množstvím záznamů.

Pomocí možnosti **Zaznamenávat textové protokoly** aktivujete ukládání protokolů do odlišného formátu:

- **Cílová složka** – složka, do které se uloží protokoly (platí pouze pro Text/CSV). Cestu ke složce můžete označit a zkopírovat si ji. Pokud si potřebujete změnit, klikněte nejprve na možnost **Vyčistit**. Každý protokol se ukládá do samostatného souboru (například ve *virlog.txt* naleznete **Zachycené hrozby**, pokud protokoly ukládáte jako prostý text).
- **Typ** – pokud vyberete **Text** jako formát souborů, protokoly budou uloženy do textového souboru, data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené středníkem ve formátu **CSV**. Pokud vyberete **Událost**, protokol bude uložen do systémového Protokolu událostí, který si můžete zobrazit v Prohlížeči událostí.
- **Odstranit všechny protokoly** – po kliknutí vymaže všechny protokoly vybrané v rozbalovacím menu **Typ**. O úspěšném vymazání protokolů budete informováni.

Zapisovat provedené změny v konfiguraci do audit logu – po aktivování této možnosti budete mít přehled o všech provedených změnách v konfiguraci produktu. Pro více informací přejděte do kapitoly Audit log.

> V rámci rychlého vyřešení problémů vás specialisté technické podpory ESET mohou požádat o zaslání protokolů. Pomocí nástroje ESET Log Collector snadno získáte diagnostické informace z počítače včetně protokolů. Pro více informací o používání ESET Log Collector navštivte ESET Databázi znalostí.

Prezentační režim

Prezentační režim je funkce navržená pro uživatele, kteří vyžadují nepřetržité používání softwaru, nechtějí být rušeni okny s oznámeními nebo upozorněními a chtějí minimalizovat používání CPU. Prezentační režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami antiviru. Zapnutím této funkce zakážete zobrazování všech vyskakujících oken a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

Prezentační režim můžete zapnout nebo vypnout v hlavním okně programu na záložce **Nastavení** > **Počítač** pomocí přepínače  nebo  vedle položky **Prezentační režim**. Zapnutý prezentační režim představuje potenciální bezpečnostní riziko, proto se ikona stav ochrany na hlavní liště změní na oranžovou barvu a zobrazí se související upozornění. V hlavním okně programu se zobrazí oranžové upozornění, že **Prezentační režim je zapnutý**.

Aktivujte možnost **Automaticky zapnout Prezentační režim při běhu aplikací zobrazených na celou obrazovku** v Rozšířených nastaveních > **Nástroje** > **Prezentační režim**, aby se prezentační režim spustil vždy, když spustíte aplikaci přes celou plochu, a zastavil se po jejím ukončení.

Můžete také aktivovat možnost **Automaticky vypínat Prezentační režim** a následně definovat interval, po jehož uplynutí se prezentační režim automaticky vypne.

Pokud je firewall v Interaktivním režimu a zapnete Prezentační režim, mohou se vyskytnout problémy s připojením do internetu. Toto může představovat problém, například pokud spouštíte hru, která se k němu připojuje. Je to způsobeno tím, že za normálních okolností by si firewall vyžádal potvrzení připojení (pokud nejsou definována žádná pravidla nebo výjimky pro spojení), ale v Prezentačním režimu jsou všechna vyskakovací okna vypnuta. Řešením je definovat pravidla nebo výjimky pro každou aplikaci, která by mohla mít konflikt s tímto chováním nebo použít jiný režim filtrování firewallu. Mějte také na paměti, že pokud při zapnutém Prezentačním režimu pracujete s aplikací nebo stránkou, která představuje potenciální riziko, pak bude tato stránka zablokována, ale nezobrazí se žádné vysvětlení nebo varování, protože jsou vypnuté všechny akce vyžadující zásah uživatele.

Diagnostika

Diagnostika poskytuje výpisy ze selhání běhu procesů programu ESET (například ekrn). Pokud aplikace spadne, vygeneruje se výpis, tzv. dump. Ten může pomoci vývojářům při ladění a opravě různých problémů v ESET Endpoint Security.

Z rozbalovacího menu **Typ výpisu** vyberte jednu z níže uvedených možností:

- Vyberte možnost **Žádný** pro vypnutí této funkce.
- **Minimální** (výchozí) – zaznamená nejmenší sadu užitečných informací, které mohou pomoci identifikovat důvod, proč se aplikace nečekaně zastavila. Tento typ výpisu může být užitečný, pokud jste omezeni volným místem na disku. Nicméně, kvůli omezenému množství zahrnutých informací, chyby, které nebyly způsobeny přímo vláknem (thread) běžícím v době problému, nemusí být objeveny analýzou tohoto souboru.
- **Úplný** – zaznamená celý obsah systémové paměti, když se aplikace nečekaně zastaví. Kompletní výpis z paměti může obsahovat data procesů, které běžely v době, kdy byl výpis vytvořen.

Cílová složka – místo, kam se vygeneruje výpis při pádu.

Otevřete složku diagnostiky – klikněte na **Otevřít** k zobrazení obsahu výše uvedené složky v novém okně *Průzkumníku Windows*.

Vytvořit diagnostický dump – po kliknutí na tlačítko **Vytvořit** se do **cílové složky** vygeneruje soubor s výpisem obsahu paměti.

Rozšířené protokolování

Aktivovat rozšířené protokolování antispamového jádra – po aktivování této možnosti se zaznamenají všechny události v průběhu kontroly zpráv. Toto nám pomůže diagnostikovat a odstranit potíže s antispamovým jádrem.

Aktivovat rozšířené protokolování skeneru – po aktivování této možnosti se do protokolu zaznamenají všechny události, které vznikly při běhu rezidentní ochrany souborového systému nebo volitelné kontrole počítače.

Aktivovat diagnostické protokolování správy zařízení – po aktivování této možnosti se do souboru zapíší detailní informace z běhu správy zařízení. Toto nám pomůže diagnostikovat a odstranit potíže se správou zařízení.

Aktivovat rozšířené protokolování Direct Cloud – po aktivování této možnosti se do souboru zaznamená veškerá komunikace mezi produktem a servery Direct Cloud.

Aktivovat rozšířené protokolování Ochrany dokumentů – po zapnutí se zaznamenají veškeré události související s modulem Ochrana dokumentů. Toto pomůže vývojářům při diagnostice a řešení problémů.

Aktivovat rozšířené protokolování ochrany poštovních klientů – po aktivování této možnosti se do souboru zapíší detailní informace z běhu ochrany poštovních klientů a jejího doplňku. Toto pomůže vývojářům při diagnostice a řešení problémů s touto součástí programu.

Aktivovat diagnostické protokolování jádra – po aktivování této možnosti se do souboru zapíší detailní informace z běhu jádra produktu ESET (služby ekrn), což nám pomůže při diagnostice a řešení problémů.

Aktivovat diagnostické protokolování licence – zaznamená se veškerá komunikace produktu s aktivačními a licenčními servery společnosti ESET.

Zapnout výpis paměti – po aktivování této možnosti se zaznamenají všechny události, které pomohou vývojářům při diagnostice úniku paměti (memory leaku).

Aktivovat rozšířené protokolování síťové ochrany – po aktivování této možnosti se do souboru v PCAP formátu bude zaznamenána veškerá síťová komunikace vyhodnocována firewallem. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem firewallu.

Aktivovat rozšířené protokolování kontroly síťové komunikace – zaznamenávání všech dat procházejících kontrolou síťové komunikace do souboru ve formátu PCAP, který pomůže vývojářům při diagnostice a řešení problémů souvisejících s kontrolou síťového provozu.

Aktivovat rozšířené protokolování operačního systému – po aktivování se sesbírají informace o operačním systému jako jsou spuštěné procesy, aktivita CPU a diskové operace. Toto pomůže vývojářům při diagnostice a řešení problémů s chodem programu ve vašem operačním systému (dostupné na Windows 10).

Aktivovat rozšířené protokolování push zpráv – po aktivování této možnosti se zaznamenají všechny události, které pomohou při diagnostice a řešení problémů souvisejících se zasíláním push zpráv.

Aktivovat diagnostické protokolování rezidentní ochrany souborového systému – zaznamenávají se všechny události, které se vyskytnou v rezidentní ochraně souborového systému, aby bylo možné diagnostikovat a řešit problémy.

Aktivovat rozšířené protokolování zabezpečeného prohlížeče – zaznamenávají se všechny události, které se vyskytnou v zabezpečeném prohlížeči, aby bylo možné diagnostikovat a řešit problémy.

Aktivovat rozšířené protokolování modulu aktualizace – po aktivování této možnosti se do souboru zapíší detailní informace o průběhu aktualizace programu. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem zajišťujícím aktualizaci programu.

Zapnout rozšířené protokolování Správy zranitelností a záplat – všechny události se zaznamenávají do Správy zranitelností a záplat. Toto nastavení se zobrazí pouze v případě, že je ve vašem prostředí povolena Správa zranitelností a záplat (povoluje se v ESET PROTECT Cloud).

Aktivovat rozšířené protokolování filtrování obsahu webu – po aktivování této možnosti se do souboru zapíší

detailní informace z běhu filtrování obsahu webu. To může vývojářům pomoci diagnostikovat a opravit problémy související s filtrováním obsahu webu.

Protokoly se nachází ve složce *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Technická podpora

Pokud zakládáte z ESET Endpoint Security požadavek na Technickou podporu ESET, můžete zjednodušit práci našim expertům odesláním konfiguračních dat systému. Z rozbalovací nabídky **Odeslat konfiguraci systému** zvolte možnost **Odeslat vždy** pro automatické odeslání dat nebo **Dotázat se před odesláním**, pokud chcete mít před založením požadavku možnost volby.

Připojení

V určitých sítích může proxy server zprostředkovávat komunikaci mezi vaším zařízením a internetem. Pokud používáte proxy server, je třeba provést následující nastavení. V opačném případě se ESET Endpoint Security a jeho moduly nemohou automaticky aktualizovat. V ESET Endpoint Security je nastavení proxy serveru k dispozici ve dvou různých sekcích v Rozšířeném nastavení.

V prvním případě můžete nastavení serveru konfigurovat v části Rozšířená nastavení > **Připojení** > **Proxy server**. Tato nastavení specifikují globální nastavení proxy serveru a tyto parametry se použijí pro jakýkoliv modul ESET Endpoint Security. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

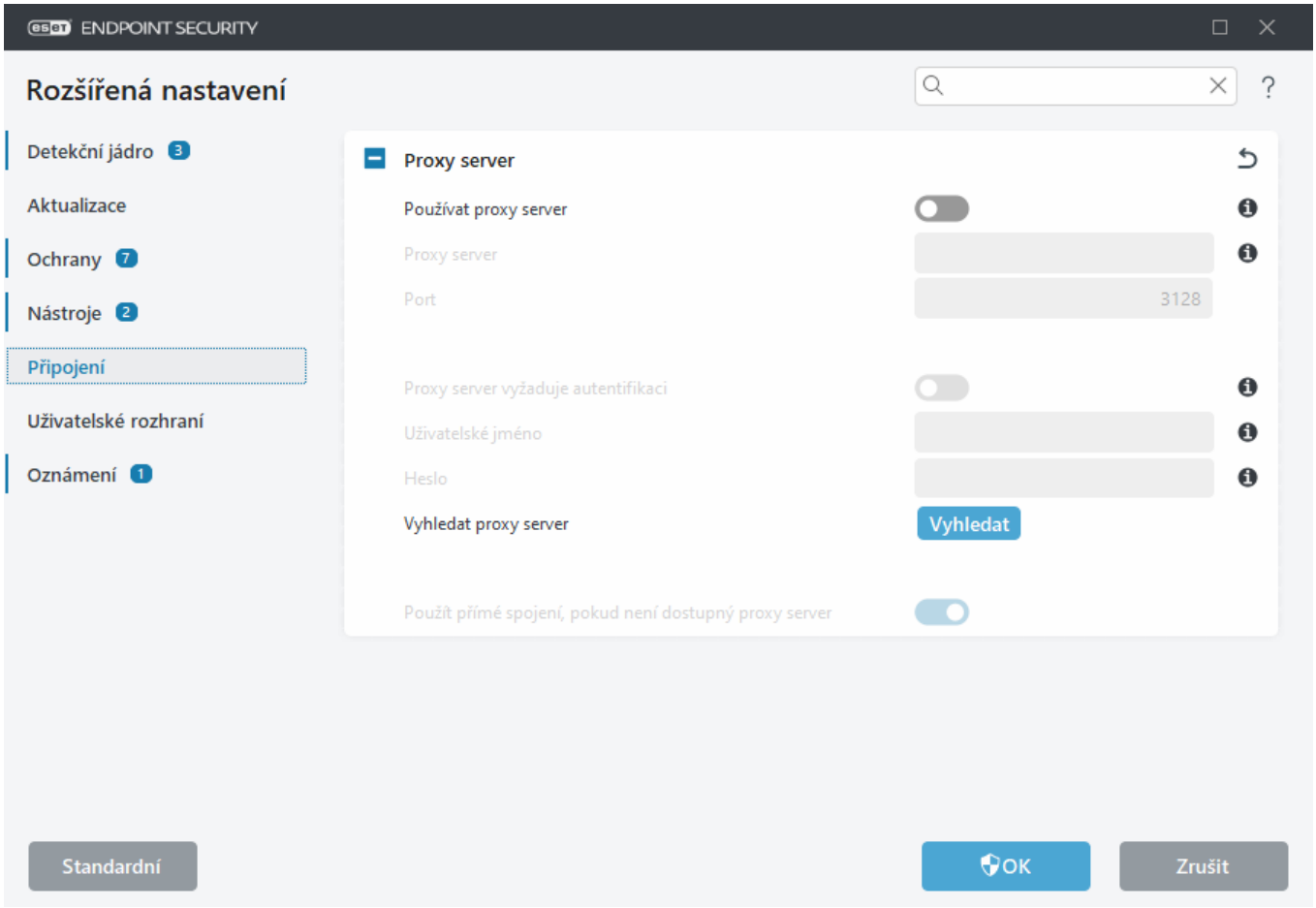
Chcete-li zadat globální nastavení proxy serveru, povolte možnost **Používat proxy server** a zadejte adresu **proxy serveru** spolu s číslem **portu** proxy serveru.

Pokud komunikace s proxy serverem vyžaduje ověření, vyberte možnost **Proxy server vyžaduje ověření** a do příslušných polí zadejte platné **uživatelské jméno** a **heslo**. Pro získání automatického nastavení proxy serveru můžete kliknout na tlačítko **Vyhledat**. Chcete-li v operačním systému najít nastavení proxy serveru, stiskněte klávesovou zkratku **Windows + I** a klikněte na **Síť & Internet** > **Proxy server**. ESET Endpoint Security zkopíruje parametry zadané v možnostech internetu pro Internet Explorer nebo Google Chrome.

> V nastavení **proxy serveru** musíte ručně zadat své uživatelské jméno a heslo.

Použít přímé spojení, pokud není dostupný proxy server – pokud máte nastaveno, že se má ESET Endpoint Security připojovat k serverům ESET prostřednictvím proxy, po aktivování této možnosti se produkt pokusí navázat spojení bez použití proxy.

Nastavení proxy serveru lze provést také v Rozšířeném nastavení > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení** výběrem možnosti **Připojení prostřednictvím proxy serveru** v rozbalovací nabídce **Režim proxy**. Tato konfigurace platí pouze pro aktualizace a doporučuje se pro notebooky, které přijímají aktualizace modulů ze vzdálených umístění. Další informace naleznete v kapitole Pokročilé nastavení aktualizace.



Uživatelské rozhraní

Chcete-li nakonfigurovat chování grafického uživatelského rozhraní (GUI) programu, otevřete Rozšířená nastavení > **Uživatelské rozhraní**.

V části prvky uživatelského rozhraní můžete přizpůsobit vzhled rozhraní a množství použitých efektů.

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu, stejně tak jeho odinstalaci, si v sekci Přístup k nastavení nastavte heslo.

Možnosti pro změnu chování systémových oznámení, upozornění na detekce a stavů aplikace naleznete v sekci Oznámení.

Prezentační režim je vhodný pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni oznámeními a chtějí minimalizovat veškeré nároky na zatížení procesoru.

Dále se můžete podívat na to, jak minimalizovat uživatelské rozhraní ESET Endpoint Security (užitečné v případě spravovaných prostředí).

Prvky uživatelského rozhraní

Uživatelské rozhraní programu ESET Endpoint Security si můžete přizpůsobit svým potřebám. Tyto možnosti jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

V sekci **Prvky uživatelského rozhraní** můžete přizpůsobit, jaké grafické prvky programu se zobrazí. V rozbalovacím menu **Režim spuštění** jsou k dispozici následující režimy:

Úplný – zobrazí se úplné grafické rozhraní.

Minimální – grafické rozhraní běží, ale uživateli jsou zobrazována pouze oznámení.

Ruční – grafické rozhraní se nespustí automaticky při přihlášení. Může jej kdykoli spustit jakýkoli uživatel.

Tichý – uživateli se nezobrazí žádná oznámení ani upozornění. Grafické rozhraní může spustit pouze administrátor. Tichý režim můžete použít ve spravovaných prostředích nebo v případě, kdy grafické rozhraní zpomaluj běh počítače nebo způsobuje jiné problémy.

> Po aktivaci tichého režimu a restartování počítače se uživateli budou zobrazovat pouze oznámení. Pro obnovení grafického rozhraní klikněte na Start > **Všechny programy** > **ESET** > ESET Endpoint Security a spusťte aplikaci jako administrátor. Případně můžete režim zobrazení změnit prostřednictvím politiky definované v ESET PROTECT.

Barevný režim – v této části zvolte barevné schéma, ve kterém se bude uživatelské rozhraní ESET Endpoint Security zobrazovat:

- **Stejný jako barva systému** – rozhraní ESET Endpoint Security se zobrazí ve stejném barevném schématu, jako uživatelské rozhraní vašeho operačního systému
- **Tmavý** – ESET Endpoint Security bude zobrazen v tmavém režimu
- **Světlý** – ESET Endpoint Security bude zobrazen ve světlém režimu

> V pravém horním rohu hlavního okna programu si můžete navolit barevný režim, ve kterém se vám bude zobrazovat uživatelské rozhraní ESET Endpoint Security.

Pomocí možnosti **Zobrazit úvodní obrázek při startu** zapnete nebo vypnete zobrazování úvodního obrázku při spouštění ESET Endpoint Security.

Pokud chcete, aby ESET Endpoint Security přehrával zvuky při důležitých událostech (například při detekci hrozby či dokončené kontrole), zapněte možnost **Používat zvuková upozornění**.

Integrovat do kontextového menu – pomocí této možnosti integrujete ovládací prvky programu ESET Endpoint Security do kontextového menu.

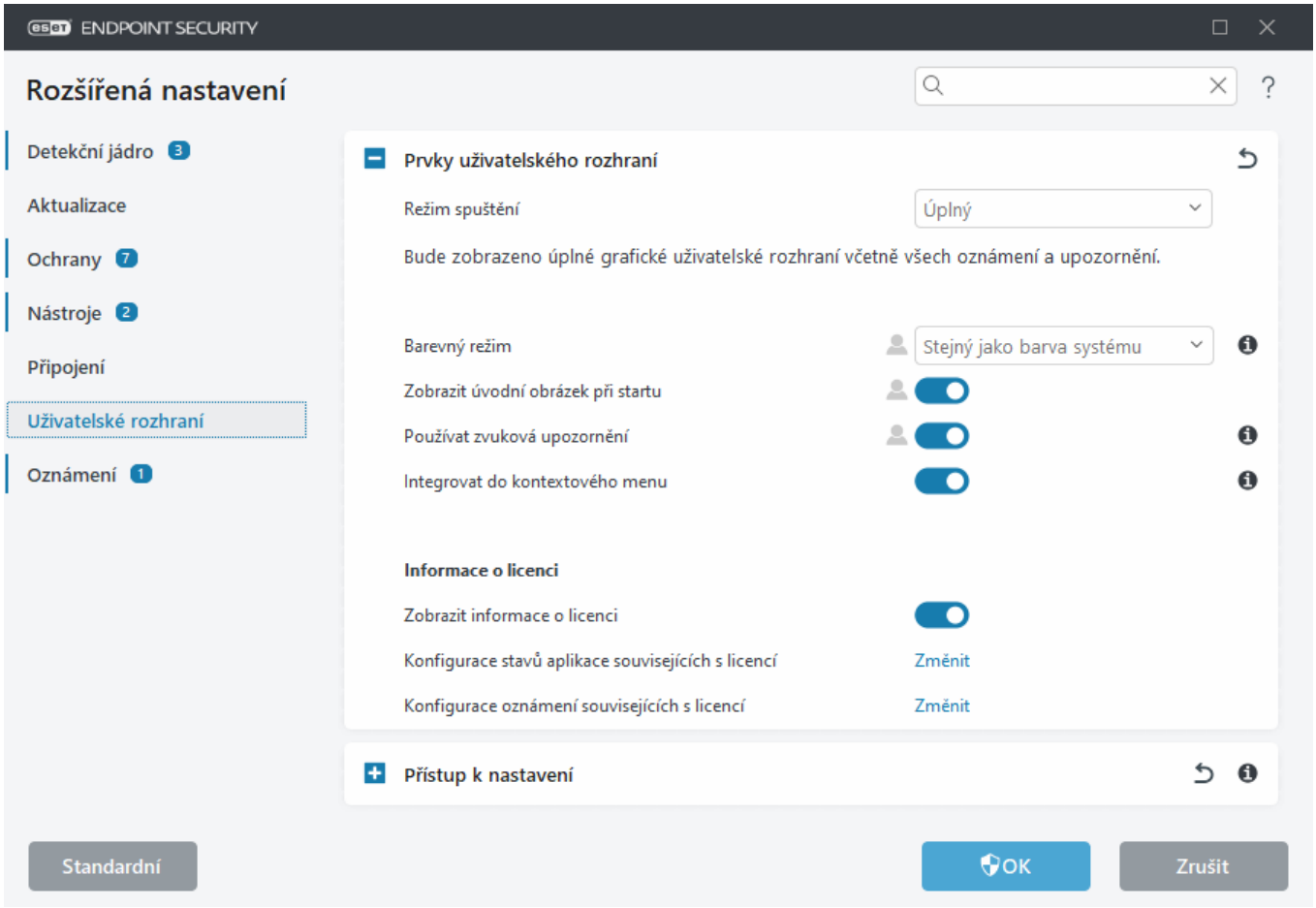
Informace o licenci

Zobrazit informace o licenci – pokud deaktivujete tuto možnost, na záložce **Stav ochrany** a **Nápověda podpora** se nezobrazí informace o licenci.

Konfigurace stavů aplikace souvisejících s licencí – zobrazí seznam stavů aplikace souvisejících s licencí.

Zobrazit informace o licenci a upozornění – pokud deaktivujete tuto možnost, upozornění se zobrazí pouze v případě, kdy se blíží konec platnosti licence/licence vypršela.

> Nastavení týkající se zobrazování informací se aplikují, ale v produktu ESET Endpoint Security aktivovaném prostřednictvím MSP licence nejsou dostupná.



Přístup k nastavení

Správné nastavení ESET Endpoint Security je velmi důležité pro celkové zabezpečení systému. Neoprávněná změna může vést ke snížení stability a ochrany. Prevencí proti neoprávněným změnám v ESET Endpoint Security je možnost nastavení hesla. Nastavení přístupu lze konfigurovat v Rozšířeném nastavení > **Uživatelské rozhraní** > **Přístup k nastavení**.

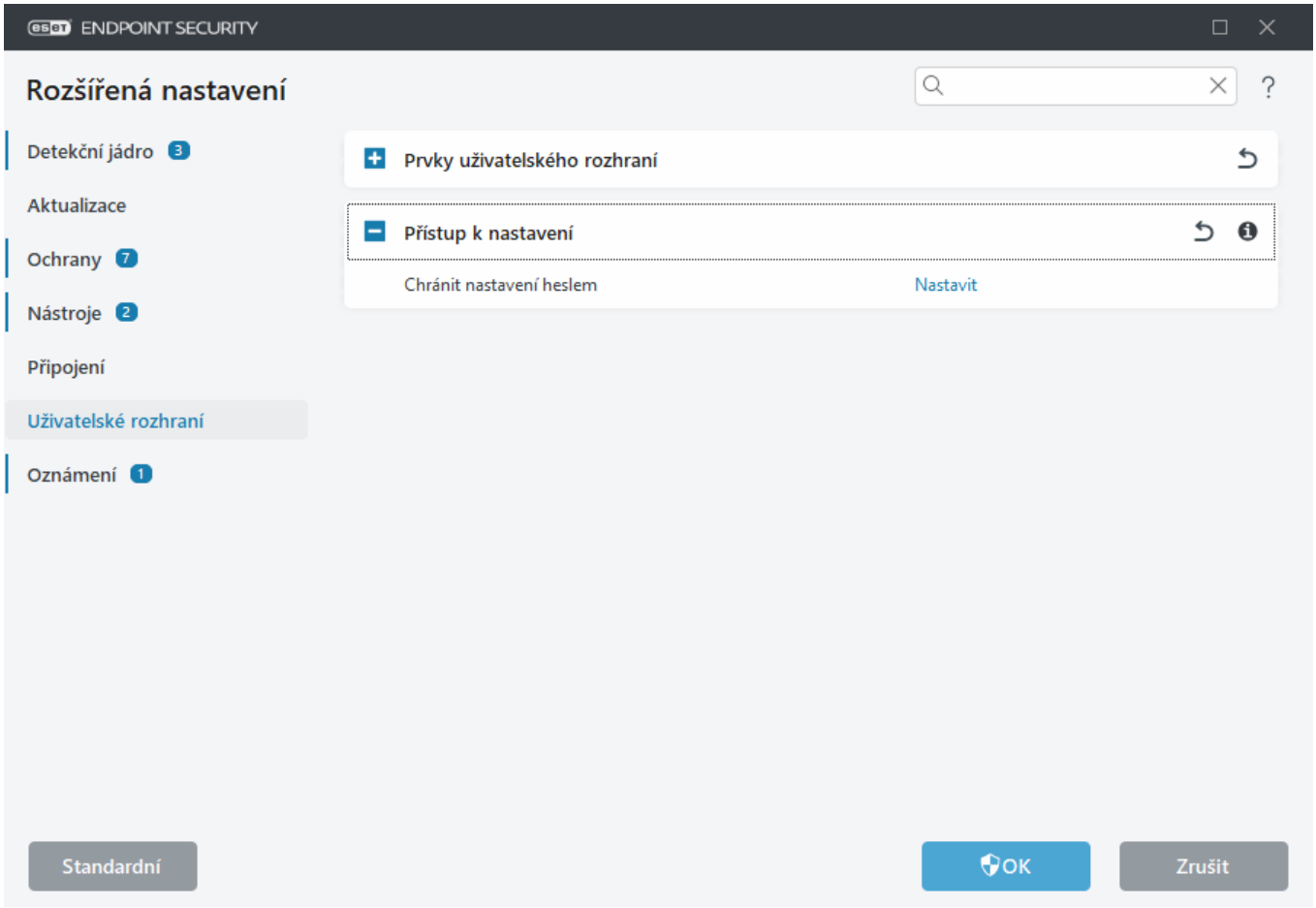
Heslo jako prvek zabezpečení proti neoprávněnému nastavení ESET Endpoint Security nebo odinstalaci nastavte, případně změňte kliknutím na **Nastavit** vedle položky **Chránit nastavení heslem**.

Pro změnu hesla klikněte na **Změnit heslo** vedle položky **Chránit nastavení heslem**.

Pro odstranění hesla klikněte na **Odstranit** vedle položky **Chránit nastavení heslem**.

Spravované prostředí

Administrátor může vytvořit politiku, a na spravovaných počítačích hromadně nastavit heslo pro ochranu nastavení produktu ESET Endpoint Security. Pro vytvoření politiky postupuje podle kroků uvedených v kapitoleOchrana produktu heslem.



Heslo pro přístup do Rozšířeného nastavení

Rozšířená nastavení ESET Endpoint Security doporučujeme ochránit před neoprávněnými změnami heslem. Heslo zadejte do polí **Nové heslo** a **Potvrzení hesla**. Klikněte na tlačítko **OK**.

Spravované prostředí

Administrátor může vytvořit politiku, a na spravovaných počítačích hromadně nastavit heslo pro ochranu nastavení produktu ESET Endpoint Security. Pro vytvoření politiky postupuje podle kroků uvedených v kapitoleOchrana produktu heslem.

Nespravované prostředí

Při změně stávajícího hesla:

1. Staré heslo zadejte do pole **Původní heslo**.
2. Nové heslo zadejte dvakrát do polí **Nové heslo** a **Potvrzení hesla**.
3. Klikněte na tlačítko **OK**.

Nastavené heslo bude následně vyžadováno při každé změně nastavení produktu ESET Endpoint Security.

Pokud heslo zapomenete, prostudujte si článek Obnovení hesla chránícího přístup do nastavení v produktech ESET Endpoint.

Pokud jste ztratili licenční klíč a potřebujete ověřit datum platnosti nebo jiné informace týkající se vaší licence k

produktu ESET Endpoint Security, postupujte podle kroků na stránce Ztratili jste licenční údaje k produktu ESET?

Heslo

Pro zabránění neautorizovaných změn v konfiguraci ESET Endpoint Security můžete přístup do rozšířeného nastavení produktu ochránit heslem.

Nouzový režim

Při spuštění grafického prostředí ESET Endpoint Security v nouzovém režimu se zobrazí dialog s informací, že program byl spuštěn v nouzovém režimu. Protože v nouzovém režimu je běh všech programů omezen, není možné spustit grafické prostředí ESET Endpoint Security stejně jako ve standardním režimu.

Zobrazené okno vám umožní spustit kontrolu počítače. Pokud chcete zkontrolovat počítač na přítomnost škodlivého kódu, vyberte možnost **Ano**.

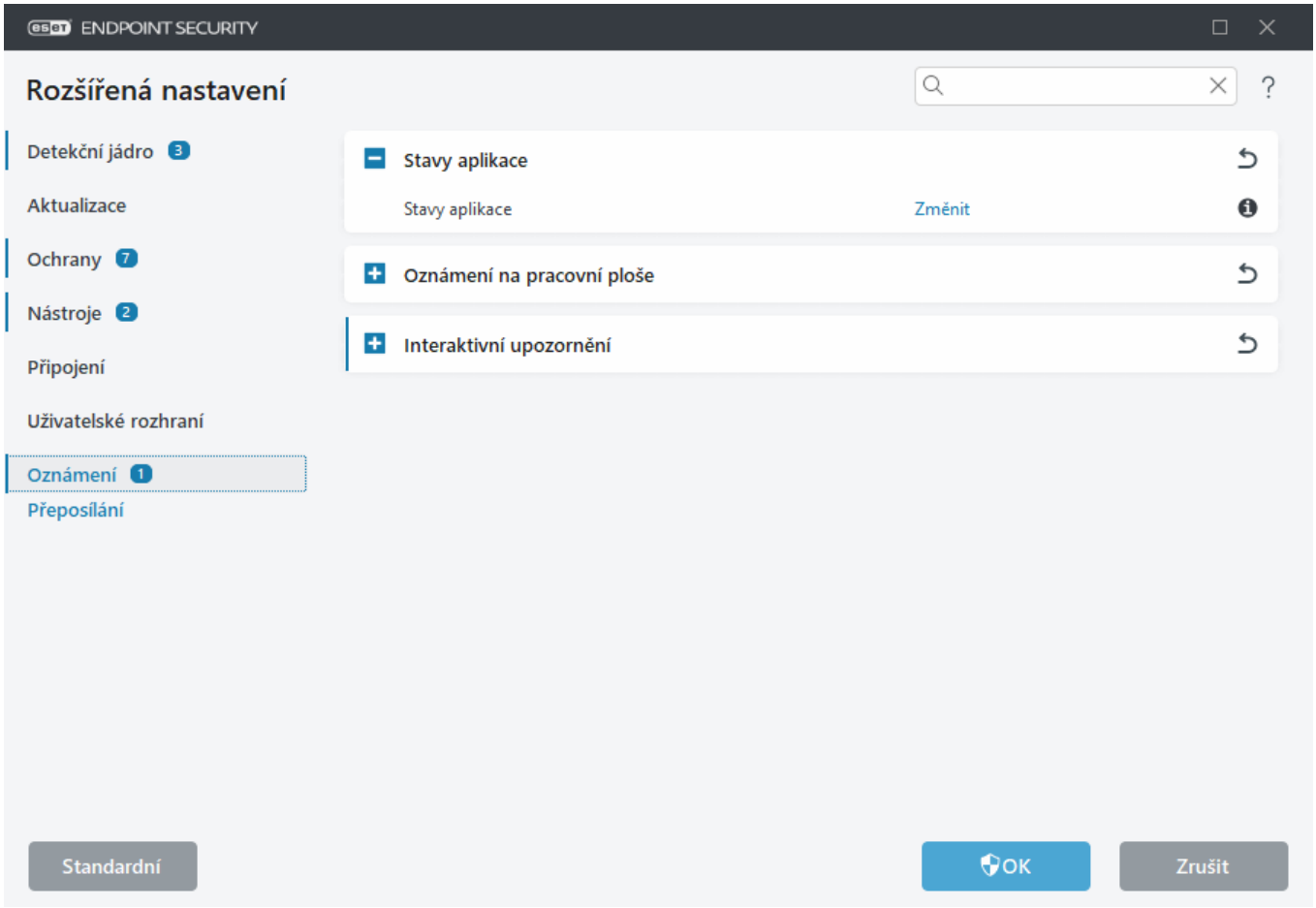
Po zahájení kontroly se otevře samostatné okno a pro kontrolu počítače se použijí přednastavené parametry ESET Endpoint Security.

Pokud vyberete možnost **Ne**, dialogové okno ESET Endpoint Security se zavře a neprovede se žádná akce.

Oznámení

Chcete-li spravovat oznámení ESET Endpoint Security, otevřete Rozšířená nastavení > **Oznámení**. V této části můžete konfigurovat následující typy oznámení:

- Stavy aplikace – jedná se o oznámení, která se zobrazují v hlavním okně programu.
- Oznámení na pracovní ploše – malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami).
- Interaktivní upozornění – výstražná upozornění a informační okna, která vyžadují interakci uživatele.
- Přeposílání (e-mailová oznámení) – oznámení se zasílají e-mailem na konkrétní adresy.
- Přizpůsobení oznámení – do oznámení zobrazovaných na ploše si můžete přidat vlastní zprávu.



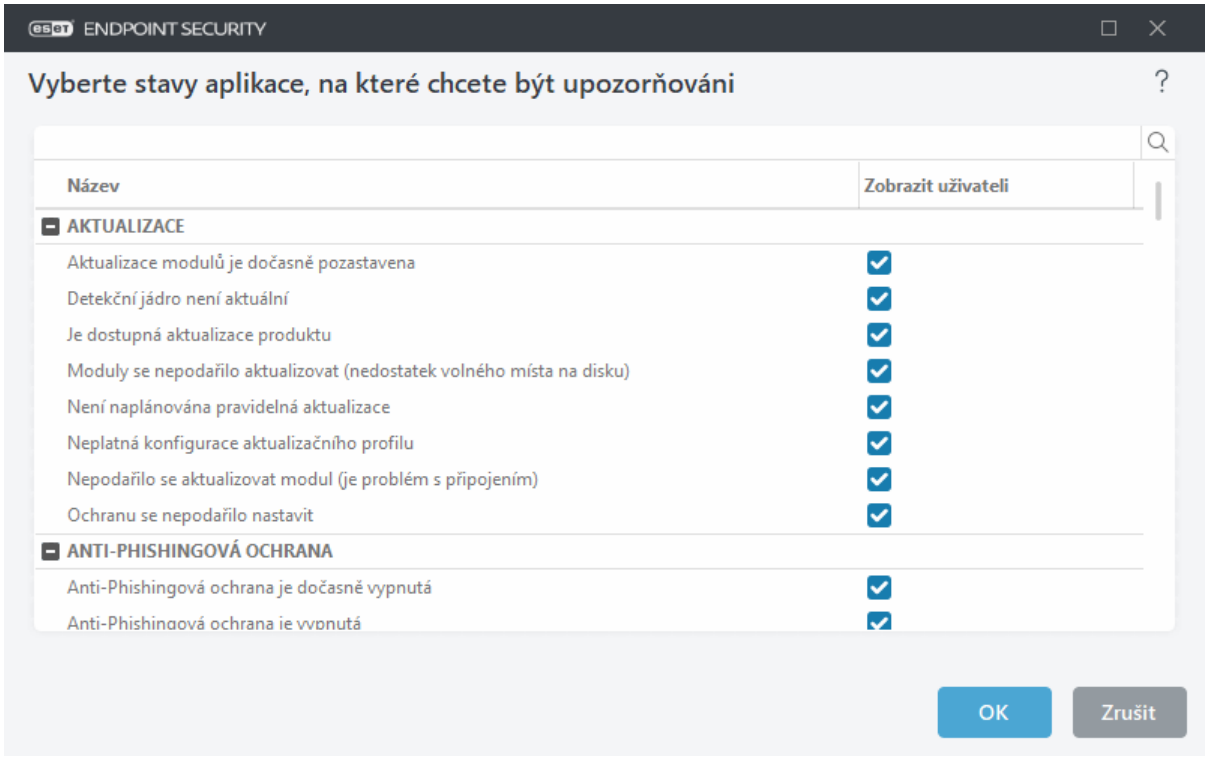
Stavy aplikace

Stavy aplikace – po kliknutí na **Změnit** se můžete rozhodnout, jaké stavy aplikace chcete zobrazovat v hlavním okně programu.

Stavy aplikace

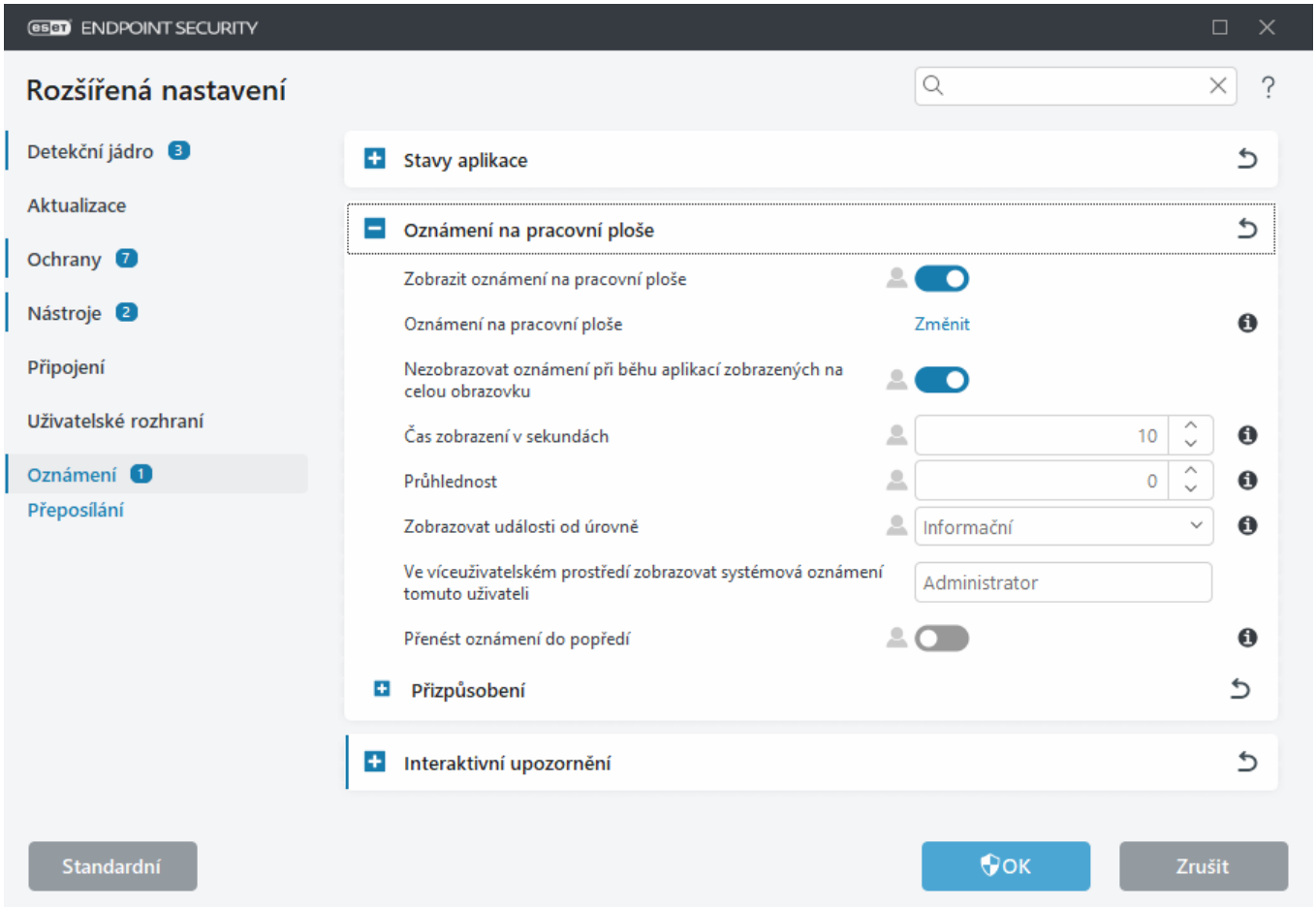
Chcete-li nakonfigurovat, které stavy aplikace se budou zobrazovat (například když pozastavíte antivirovou a antispywarovou ochranu nebo zapnete prezentační režim), otevřete Rozšířená nastavení > **Oznámení** a klikněte na **Změnit** vedle položky **Stavy aplikací**.

Mezi sledované stavy aplikace patří také, zda je produkt aktivován, a jestli nevypršela platnost licence. Prostřednictvím politik v ESET PROTECT můžete potlačit zobrazování informací uživateli a ponechat jejich zasílání pouze do konzole pro vzdálenou správu.



Oznámení na pracovní ploše

Oznámení na pracovní ploše jsou malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami). Ve výchozím nastavení se zobrazí po dobu 10 sekund a následně pomalu zmizí. Prostřednictvím nich ESET Endpoint Security primárně komunikuje s uživatelem a informuje ho o provedených aktualizacích, nově připojených zařízeních, dokončených kontrolách nebo nalezených hrozbách.



Zobrazovat oznámení na pracovní ploše – tuto možnost doporučujeme ponechat aktivní, aby vás produkt mohl informovat o nových událostech.

Oznámení aplikace – klikněte na **Změnit** a následně si vyberte oznámení, která chcete nebo nechcete zobrazovat.

Nezobrazovat oznámení při běhu aplikací zobrazených na celou obrazovku – pomocí této možnosti potlačíte zobrazení všech oznámení v režimu celé obrazovky, která nevyžadují interakci.

Čas v sekundách – nastavte dobu viditelnosti oznámení. Hodnota musí být mezi 3 a 30 sekundami.

Průhlednost – nastavte průhlednost zobrazeného oznámení v procentech. Podporovaný rozsah je od 0 (neprůhledné) do 80 (velmi průhledné).

Zobrazovat události od úrovně – nastavit úroveň závažnosti oznámení, od které chcete být informováni. V rozbalovací nabídce vyberte následující možnosti:

- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy,
- **Varování** – do protokolu se zapíší kritické chyby, chybová a varovná hlášení (například, aktualizace se nezdařila).
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například nefunkční ochrana dokumentů),
- **Kritické** – e-mailem se odešlou upozornění na kritické stavy aplikace (například problém s antivirovou ochranou nebo upozornění na infiltraci v systému).

Ve víceuživatelském prostředí posílat systémová hlášení tomuto uživateli – nastavte uživatelský účet počítače, který bude dostávat oznámení na pracovní ploše. Pokud například nepoužíváte administrátorský účet, zadejte název toho účtu, který má být o nových událostech v produktu informovaný. Definovat je možné pouze jeden uživatelský účet.

Přenést oznámení do popředí – po aktivování této možnosti se okno oznámení přesune do popředí obrazovky a bude dostupné pomocí klávesové zkratky Alt+Tab.

Přizpůsobení oznámení

V tomto dialogovém okně si můžete přizpůsobit vzhled a chování oznámení, která se zobrazují uživateli.

Použít výchozí oznámení – v patičce oznámení se zobrazí výchozí zpráva.

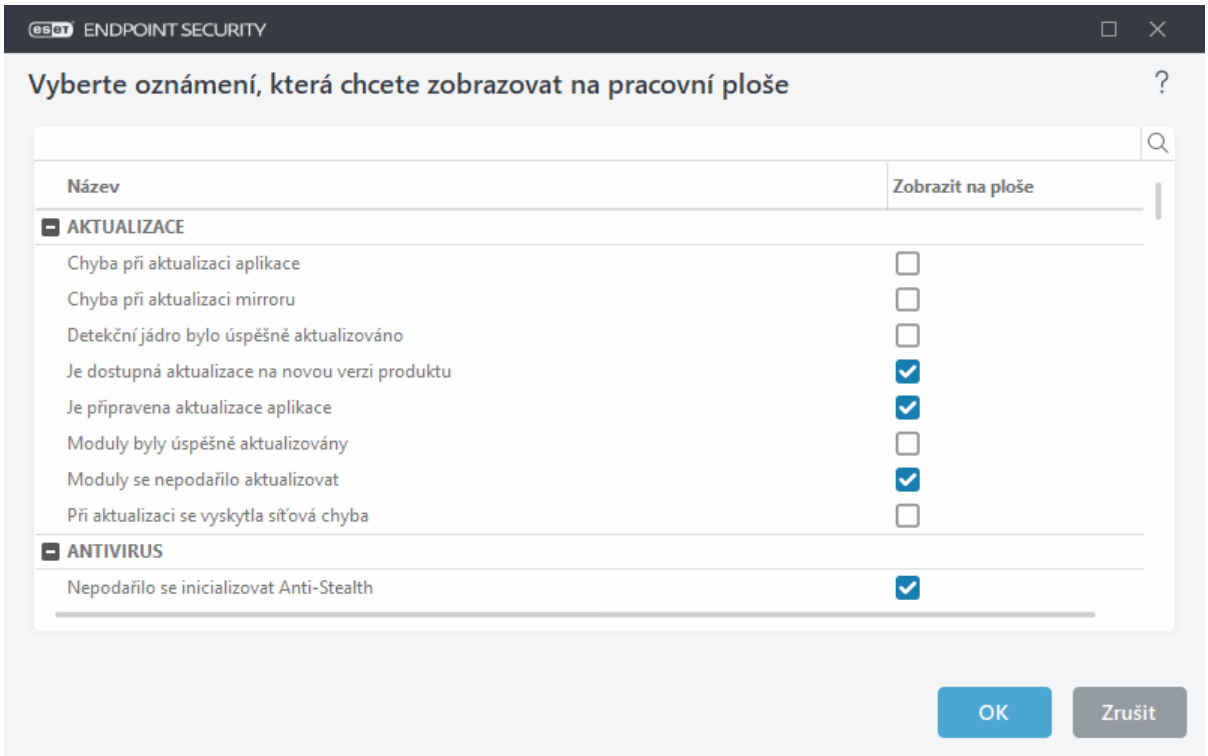
Detekce

Pomocí možnosti **Nezavírat automaticky oznámení při výskytu detekce** zůstane upozornění zobrazeno tak dlouho, dokud jej uživatel nezavře.

Pokud chcete uživateli zobrazit vlastní zprávu, deaktivujte možnost **Použít výchozí oznámení** a do pole **Zpráva při výskytu detekce** zadejte vlastní text zprávy.

Dialogové okno – Oznámení na pracovní ploše

Kdykoli se můžete rozhodnout, jaká oznámení produktu chcete zobrazovat na pracovní ploše (v pravém dolním rohu obrazovky). Otevřete si Rozšířená nastavení > **Oznámení** > **Oznámení na pracovní ploše**. Na řádku **Oznámení na pracovní ploše** klikněte na **Změnit** a následně v zobrazeném dialogovém okně jednotlivá oznámení zapněte pomocí zaškrtávacího pole ve sloupci **Zobrazit na ploše**.



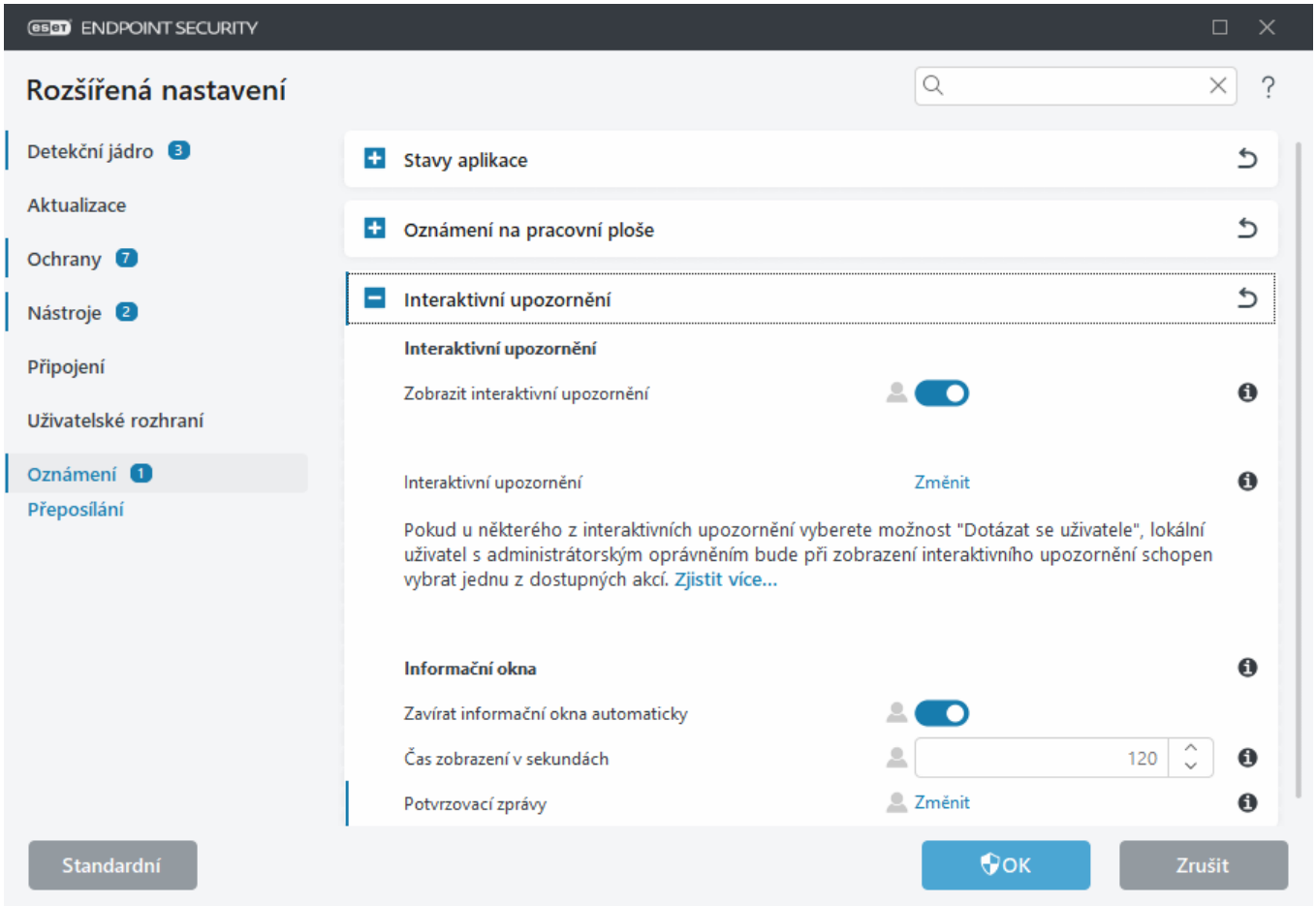
Abyste mohli konfigurovat oznámení **Soubor byl analyzován** a **Soubor nebyl analyzován** související se zasíláním vzorků do služby ESET LiveGuard, v sekci Proaktivní ochrana musíte mít nastavenou možnost **Blokovat spuštění do obdržení výsledku analýzy**.

Interaktivní upozornění

Hledáte informace o běžných upozorněních a oznámeních?

- Nalezena hrozba
- Přístup na adresu byl zablokován
- Produkt není aktivován
- Je dostupná aktualizace
- Informace o aktualizaci nejsou konzistentní
- Řešení problémů pro chybové hlášení "Moduly se nepodařilo aktualizovat"
- "Soubor je poškozen" nebo "Nepodařilo se přejmenovat soubor"
- Certifikát webové stránky byl zamítnut
- Zablokována síťová hrozba
- Přístup k souboru je blokován z důvodu analýzy

V **Rozšířeném nastavení** v sekci Oznámení > **Interaktivní upozornění** můžete nastavit, jak se má ESET Endpoint Security zachovat, pokud bude při detekci vyžadovat interakci uživatele (například při pokusu o přístup na potenciálně phishingovou stránku), stejně tak způsob zobrazování informačních oken.



Interaktivní upozornění

Vypnutí možnosti **Zobrazit interaktivní upozornění** skryje všechna dialogová okna s upozorněními, včetně

informací ve webových prohlížečích. Tuto možnost je vhodné vypnout pouze v určitých situacích.

- V případě samostatných instalací doporučujeme toto nastavení ponechat beze změny (standardně zapnuto).
- Ve spravovaných prostředích ponechte toto nastavení zapnuté a vyberte si akce, ve kterých chcete uživateli zobrazitinteraktivní upozornění.

Interaktivní upozornění – klikněte na **Změnit** pro výběr Interaktivního upozornění, která chcete zobrazovat.

Informační okna

Dobu zobrazení informačních oken nastavíte pomocí možnosti **Zavírat informační okna automaticky**. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

Čas v sekundách – nastavte dobu viditelnosti oznámení. Hodnota musí být mezi 10 a 999 sekundami.

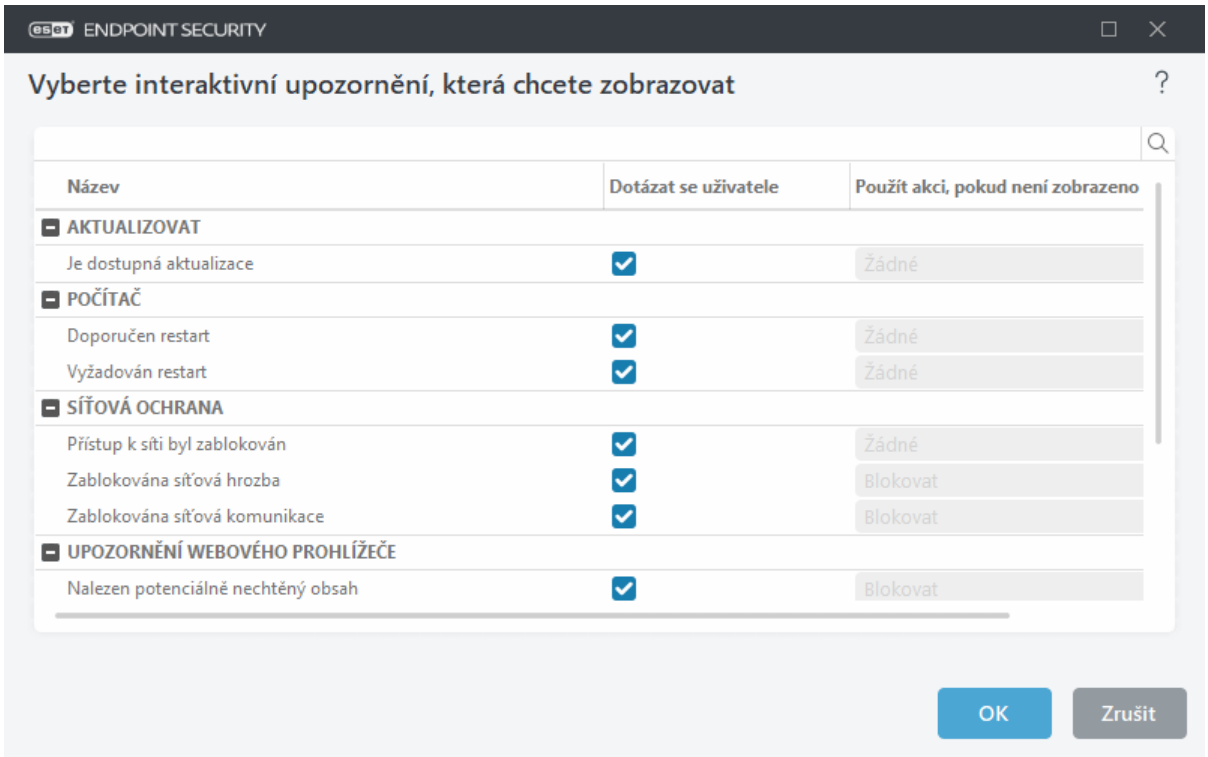
Potvrzovací zprávy – pomocí této možnosti můžete spravovat seznam potvrzovacích zpráv, jejichž zobrazování chcete povolit nebo zakázat.

Seznam interaktivních upozornění

V této sekci naleznete seznam upozornění, které může produkt ESET Endpoint Security uživateli zobrazit, pokud bude vyžadovat jeho interakci.

Pro přizpůsobení chování konfigurovatelných interaktivních upozornění přejděte v Rozšířených nastaveních do sekce **Oznámení** > **Interaktivní upozornění** a na řádku **Interaktivní upozornění** klikněte na odkaz **Změnit**.

> Tuto funkci mohou využití administrátoři ve spravovaných prostředích k tomu, aby deaktivoval možnost **Dotázat se uživatele** a definovali akci, kterou má produkt při zobrazení interaktivního upozornění automaticky provést.



Pro vysvětlení jednotlivých interaktivních upozornění se podívejte do relevantních kapitol v této příručce:

Výměnná média

- Rozpoznáno nové zařízení

Zabezpečený prohlížeč

- Umožnit pokračování ve výchozím prohlížeči

Síťová ochrana

- Přístup k síti byl zablokován – toto upozornění se zobrazí v případě, kdy byl počítač **Izolován od sítě** prostřednictvím klientské úlohy zaslané z ESET PROTECT.
- Zablokována síťová komunikace
- Zablokována síťová hrozba

Upozornění webového prohlížeče

- Nalezen potenciálně nechtěný obsah
- Webová stránka byla zablokována z důvodu výskytu phishingu

Počítač

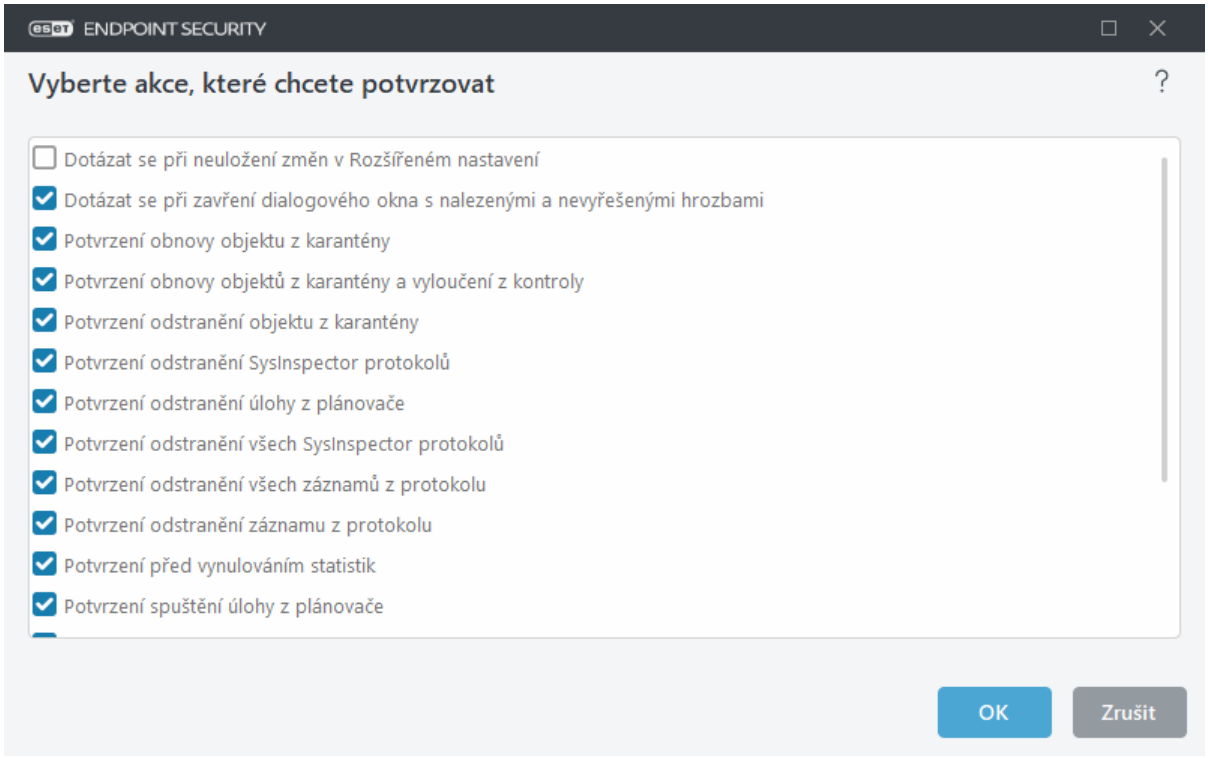
Při výskytu uvedených upozornění se změní podbarvení uživatelského rozhraní:

- Restartovat počítač (vyžadováno)
- Restartovat počítač (doporučeno)

> V seznamu interaktivních upozornění nenaleznete dialogová okna týkající se Detekčního jádra, modulu HIPS, anebo Firewallu – jejich chování můžete ovlivnit v možnostech konfigurace dané funkce.

Potvrzovací zprávy

Pro přizpůsobení potvrzovacích zpráv produktu přejděte v Rozšířených nastaveních do sekce **Oznámení** > **Interaktivní upozornění** a na řádku **Potvrzovací zprávy** klikněte na odkaz **Změnit**.



V tomto dialogovém okně můžete upravit zobrazování zpráv, které ESET Endpoint Security zobrazí před provedením akce. Pro jejich aktivaci nebo deaktivaci použijte zaškrtávací pole na daném řádku.

Pro více informací o konkrétní funkci související s potvrzovacími zprávami klikněte na odkaz:

- Potvrzení odstranění ESET SysInspector protokolů
- Potvrzení odstranění všech ESET SysInspector protokolů
- Potvrzení odstranění objektu z karantény
- Dotázat se při neuložení změn v Rozšířeném nastavení
- Dotázat se při zavření dialogového okna s nalezenými a nevyřešenými hrozbami
- Potvrzení odstranění záznamu z protokolu
- Potvrzení odstranění úlohy z plánovače
- Potvrzení odstranění všech záznamů z protokolu
- Potvrzení před vynulováním statistik
- Potvrzení obnovení objektu z karantény
- Potvrzení obnovení objektů z karantény a vyloučení z kontroly
- Potvrzení spuštění úlohy z plánovače
- Zobrazit výsledek antispamové kontroly
- Zobrazit oznámení o výsledku antispamové kontroly provedené v poštovním klientovi
- Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovních klientů Outlook Express a Windows Mail
- Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Windows Mail
- Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Microsoft Outlook

Konflikt v rozšířeném nastavení

Tato chyba může nastat, pokud některá komponenta (např. HIPS nebo Firewall) a uživatel vytvářejí pravidla v interaktivním nebo učícím režimu současně.

Před vytvořením vlastním pravidel přepněte režim filtrování na **automatický**. Pro více informací přejděte do kapitoly učící režim firewallu. Pro více informací přejděte do kapitoly HIPS a režim filtrování.

Umožnit pokračování ve výchozím prohlížeči

Konkrétní interaktivní upozornění zobrazí pouze v případě výskytu chyby při spouštění Zabezpečeného prohlížeče.

Vyžadován restart

Po aktualizaci ESET Endpoint Security na novou verzi nebo po aplikaci změn prostřednictvím Správy zranitelností a záplat je nutné zařízení restartovat. Nové verze ESET Endpoint Security opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů.

Pro restartování počítače klikněte na **Restartovat nyní**. Pokud plánujete restartovat počítač později, klikněte na **Připomenout později**. Restart zařízení můžete provést ručně v hlavním okně programu na záložce **Stav ochrany**.

Pro deaktivování zobrazování upozornění "Doporučen restart" a "Vyžadován restart" postupujte podle níže uvedených kroků:

1. Otevřete si **Rozšířená nastavení** (F5) a přejděte do sekce **Oznámení** > **Interaktivní upozornění**.
2. Na řádku **Interaktivní upozornění** klikněte na **Změnit**. V zobrazeném dialogovém okně v sekci **Počítač** odškrtněte možnost **Restartovat počítač (vyžadováno)** a **Restartovat počítač (doporučeno)**.
3. Pro uložení klikněte dvakrát na tlačítko **OK**.
4. Uvedená upozornění se již následně nebudou na stanici zobrazovat.
5. Alternativně můžete deaktivovat upozornění **Vyžadován restart počítače** a **Doporučen restart počítače** jako stavy aplikace, které se zobrazují v hlavním okně programu ESET Endpoint Security.

Doporučen restart

Po aktualizaci ESET Endpoint Security na novou verzi je vyžadován restart počítače. Nové verze ESET Endpoint Security opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů.

Pro restartování počítače klikněte na **Restartovat nyní**. Pokud plánujete restartovat počítač později, klikněte na **Připomenout později**. Restart zařízení můžete provést ručně v hlavním okně programu na záložce **Stav ochrany**.

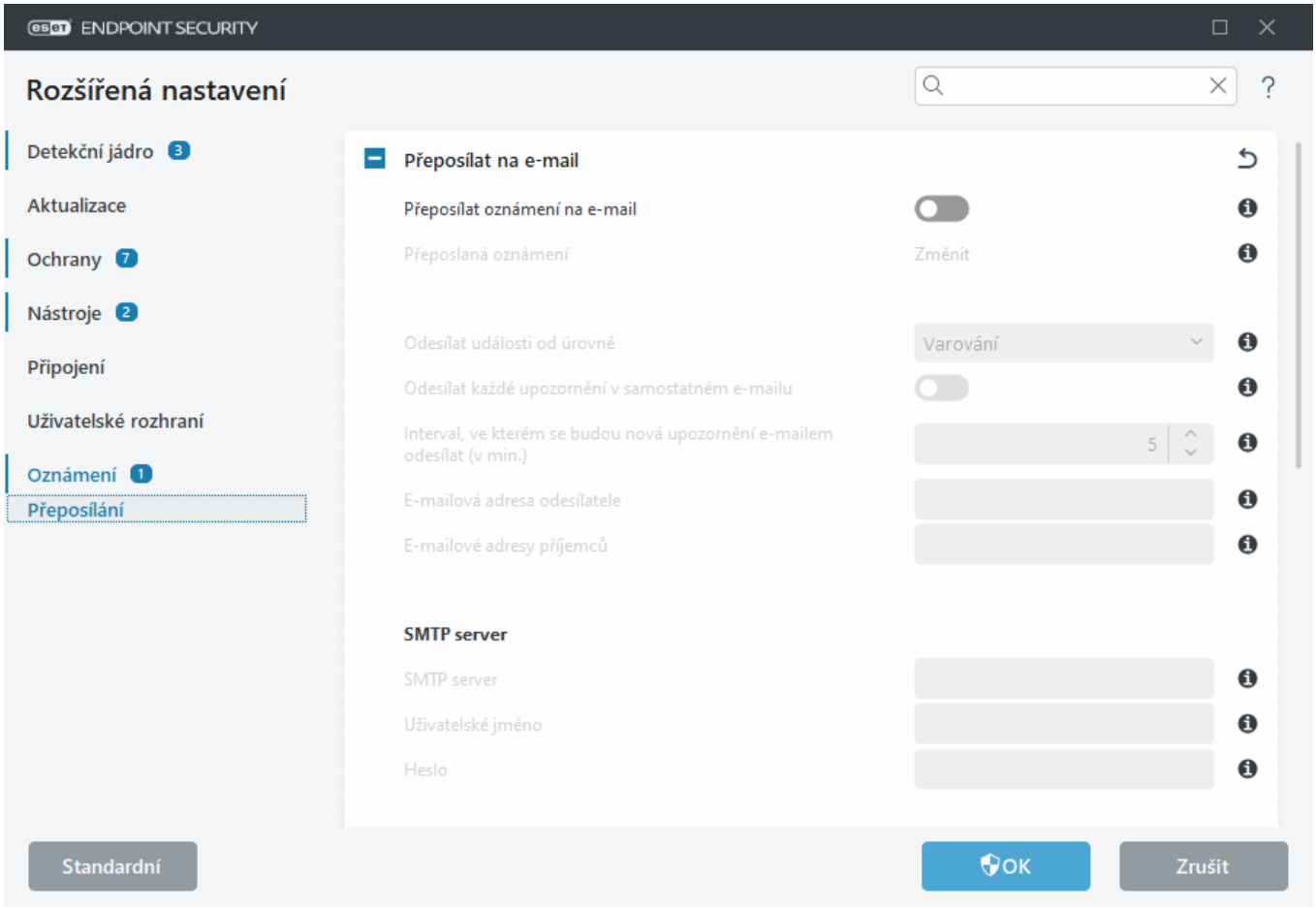
Pro deaktivování zobrazování upozornění "Doporučen restart" a "Vyžadován restart" postupujte podle níže uvedených kroků:

1. Otevřete si **Rozšířená nastavení** (F5) a přejděte do sekce **Oznámení** > **Interaktivní upozornění**.
2. Na řádku **Interaktivní upozornění** klikněte na **Změnit**. V zobrazeném dialogovém okně v sekci **Počítač** odškrtněte možnost **Restartovat počítač (vyžadováno)** a **Restartovat počítač (doporučeno)**.
3. Pro uložení klikněte dvakrát na tlačítko **OK**.
4. Uvedená upozornění se již následně nebudou na stanici zobrazovat.
5. Alternativně můžete deaktivovat upozornění **Vyžadován restart počítače** a **Doporučen restart počítače** jako stavy aplikace, které se zobrazují v hlavním okně programu ESET Endpoint Security.

Přeposílání

ESET Endpoint Security dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pro aktivování zaslání oznámení e-mailem otevřete Rozšířená nastavení > **Oznámení** > **Přeposílání** > **Přeposílat na e-mail** a zapněte možnost **Přeposílat oznámení na e-mail**.

Přeposlaná oznámení – po kliknutí si vyberte, která oznámení zobrazená na pracovní ploše se mají přeposílat také na e-mail.



Odesílat události od úrovně – specifikuje, od které úrovně důležitosti se budou upozornění na události odesílat.

- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy,
- **Varování** – do protokolu se zapíší kritické chyby, chybová a varovná hlášení (například, aktualizace se nezdařila).
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například nefunkční ochrana dokumentů),
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany nebo infiltraci v systému),

Odesílat každé upozornění v samostatném e-mailu – pokud je tato možnost aktivní, příjemce obdrží při výskytu události nové upozornění. Při výskytu velkého množství událostí v krátkém čase obdrží příjemce velké množství e-mailů.

Interval, ve kterém se budou nová upozornění odesílat (v min.) – interval v minutách, po jehož uplynutí bude odeslán souhrnný e-mail se všemi upozorněními na události, které se v daném intervalu vyskytly. Pokud nastavíte hodnotu na 0, upozornění bude odesláno okamžitě po jeho výskytu.

E-mailová adresa odesílatele – specifikuje adresu odesílatele, která se použije v hlavičce e-mailové zprávy.

E-mailová adresa příjemce – specifikuje adresu příjemce, která se použije v hlavičce e-mailové zprávy. Podporováno je více hodnot. Jako oddělovač použijte středník.

SMTP server

SMTP server – adresa SMTP serveru prostřednictvím kterého budou zprávy odesílány (například *smtp.provider.com:587*, pokud nespecifikujete port, použije se výchozí 25).

ESET Endpoint Security podporuje SMTP servery využívající TLS šifrování.

Uživatelské jméno a Heslo – v případě, že SMTP server vyžaduje autorizaci, musíte vyplnit tato pole pro přístup k SMTP.

E-mailová adresa odesílatele – specifikuje adresu odesílatele, která se vloží do hlavičky e-mailové zprávy.

E-mailové adresy příjemců – specifikuje adresu příjemců. Více adres oddělte středníkem (;).

Povolit TLS – umožní odesílání zpráv prostřednictvím zabezpečeného TLS spojení.

Formát zprávy

Komunikace mezi programem a vzdáleným uživatelem nebo systémovým administrátorem probíhá prostřednictvím e-mailu nebo LAN zpráv (s využitím služby Windows messaging). Výchozí formát událostí je vhodný pro většinu situací, ale v případě potřeby si jej můžete přizpůsobit. V případě potřeby si jej můžete přizpůsobit svým požadavkům.

Formát události – formát zprávy, která se zobrazí na vzdáleném počítači.

Formát zprávy s upozorněním na hrozbu – přednastavený formát zpráv je vhodný pro většinu situací. Měnit jej doporučujeme pouze v ojedinělých případech. V některých případech (například pokud máte systém pro automatické zpracování zpráv), může být potřeba změnit formát zprávy.

Znaková sada – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250, Unicode (UTF-8), ACSII 7-bit nebo (ISO-2022-JP)). To znamená, že se například znak "á" změní na "a", a neznámý symbol bude nahrazen otazníkem ("?").

Použít Quoted-printable kódování – e-mailová zpráva bude zakódována do Quoted-printable (QP) formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

Proměnné (řetězce mezi %) jsou nahrazovány aktuální informací. K dispozici jsou následující proměnné:

- **%TimeStamp%** – datum a čas události,
- **%Scanner%** – modul, který zaznamenal událost,
- **%ComputerName%** – název počítače, na kterém došlo k události,

- **%ProgramName%** – program, který způsobil událost,
- **%InfectedObject%** – název škodlivého souboru, e-mailové zprávy, apod.,
- **%VirusName%** – název infekce,
- **%Action%** – provedená akce,
- **%ErrorDescription%** – popis chyby.

Klíčová slova **%InfectedObject%** a **%VirusName%** se používají pouze v upozorněních na hrozbu. Klíčové slovo**%ErrorDescription%** se používá pouze v informačních upozorněních.

Obnovit všechna nastavení na standardní

Kliknutím na **Standardní** v Rozšířených nastaveních vrátíte zpět všechna nastavení aplikace pro všechny moduly. Tím zajistíte, že se nastavení vrátí do stavu, v jakém byla po nové instalaci.

Dále se můžete podívat do kapitoly Import a export nastavení.

Obnovit všechna nastavení v této sekci na standardní

Kliknutím na ikonu šipky obnovíte všechna nastavení v dané sekci na výchozí hodnoty definované společností ESET.

Prosím, mějte na paměti, že po kliknutí na tlačítko **Obnovit na standardní** budou všechny dosavadní změny ztraceny.

Obnovit obsah tabulek – po aktivování této možnosti se odstraní všechna ručně i automaticky přidaná pravidla, úlohy i profily.

Dále se můžete podívat do kapitoly Import a export nastavení.

Chyba během ukládání nastavení

Tato chyba značí, že nastavení nebylo správně uloženo z důvodu chyby.

To obvykle znamená, že uživatel, který se pokoušel modifikovat nastavení programu:

- nemá dostatečná přístupová oprávnění nebo nemá nezbytná oprávnění operačního systému pro úpravu konfiguračních souborů a záznamů v registru systému.
  > Pro provedení požadovaných změn se musí přihlásit administrátor systému.
- aktivoval učící režim modulu HIPS nebo firewallu, a pokouší se provádět změny v jejich nastavení.
  > Pro uložení nastavení a zabránění konfliktu ukončete Rozšířeném nastavení bez uložení změn, a zkuste změny provést znovu.

Druhou nejčastější příčinou bývá nekonzistentnost produktu, který nepracuje správně z důvodu svého poškození, a proto je nutné jej přeinstalovat.

Skener příkazového řádku

Modul antivirové ochrany produktu ESET Endpoint Security můžete spustit pomocí příkazového řádku – ručně (příkazem "ecls") nebo dávkovým souborem typu "bat".

Použití ESET skeneru z příkazového řádku:

```
ecls [MOŽNOSTI…] SOUBORY…
```

Při spouštění volitelné kontroly prostřednictvím příkazového řádku můžete použít několik parametrů a přepínačů:

Možnosti

/base-dir=SLOŽKA	načíst moduly ze SLOŽKY
/quar-dir=SLOŽKA	SLOŽKA s karanténou
/exclude=MASKA	vyloučí soubory odpovídající MASCE z kontroly
/subdir	kontrolovat podsložky (standardně)
/no-subdir	nekontrolovat podsložky
/max-subdir-level=ÚROVEŇ	podsložky kontrolovat pouze do definované ÚROVNĚ vnoření
/symlink	následovat symbolické odkazy (standardně)
/no-symlink	přeskočit symbolické odkazy
/ads	kontrolovat ADS (standardně)
/no-ads	nekontrolovat ADS
/log-file=SOUBOR	zapisovat výstup do SOUBORU
/log-rewrite	přepisovat protokol (standardně se záznamy přidají na konec souboru)
/log-console	zapisovat výstup do konzole (standardně)
/no-log-console	nezapisovat výstup do konzole
/log-all	zaznamenat do protokolu také čisté soubory
/no-log-all	nezaznamenávat do protokolu čisté soubory (standardně)
/aind	zobrazit průběh aktivity
/auto	automaticky zkontrolovat a vyléčit všechny lokální disky

Možnosti skeneru

/files	kontrolovat soubory (standardně)
/no-files	nekontrolovat soubory
/memory	kontrolovat paměť
/boots	kontrolovat boot sektory
/no-boots	nekontrolovat boot sektory (standardně)
/arch	kontrolovat archivy (standardně)
/no-arch	nekontrolovat archivy
/max-obj-size=VELIKOST	kontrolovat pouze soubory menší než VELIKOST v megabajtech (standardně 0 = neomezené)

/max-arch-level=ÚROVEŇ	archivy kontrolovat do definované ÚROVNĚ vnoření
/scan-timeout=LIMIT	archivy kontrolovat nejdéle po definovaný LIMIT v sekundách
/max-arch-size=VELIKOST	kontrolovat pouze soubory v archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/max-sfx-size=VELIKOST	kontrolovat pouze soubory v samorozbalovacích archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/mail	kontrolovat poštovní soubory (standardně)
/no-mail	nekontrolovat poštovní soubory
/mailbox	kontrolovat poštovní schránky (standardně)
/no-mailbox	nekontrolovat poštovní schránky
/sfx	kontrolovat samorozbalovací archivy (standardně)
/no-sfx	nekontrolovat samorozbalovací archivy
/rtp	kontrolovat runtime packery (standardně)
/no-rtp	nekontrolovat runtime packery
/unsafe	detekovat potenciálně zneužitelné aplikace
/no-unsafe	nedetekovat potenciálně zneužitelné aplikace (standardně)
/unwanted	detekovat potenciálně nechtěné aplikace
/no-unwanted	nedetekovat potenciálně nechtěné aplikace (standardně)
/suspicious	detekovat podezřelé aplikace (standardně)
/no-suspicious	nedetekovat podezřelé aplikace
/pattern	používat signatury (standardně)
/no-pattern	nepoužívat signatury
/heur	zapnout heuristiku (standardně)
/no-heur	vypnout heuristiku
/adv-heur	zapnout rozšířenou heuristiku (standardně)
/no-adv-heur	vypnout rozšířenou heuristiku
/ext-exclude=PŘÍPONY	vyloučit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=REŽIM	použít REŽIM léčení infikovaných objektů K dispozici jsou následující možnosti: • `none` (standardně) – automaticky se nevyléčí žádné objekty. • `standard` – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit. • `strict` – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit bez interakce uživatele (nebudete dotázání na vymazání souboru). • `rigorous` – ecls.exe automaticky odstraní soubor bez pokusu o jeho vyléčení. • `delete` – ecls.exe automaticky odstraní soubor bez pokusu o jeho vyléčení, ale neodstraní se důležité systémové soubory Windows.
/quarantine	uložit infikované soubory (při léčení) do karantény (doplňková akce při léčení souborů)
/no-quarantine	neukládat infikované soubory do karantény

Všeobecné možnosti

/help	zobrazit tuto nápovědu a ukončit
/version	zobrazit informaci o verzi a ukončit
/preserve-time	zachovat čas přístupu k souborům

Návratové hodnoty

0	nenalezeny žádné hrozby
1	hrozba nalezena a vyléčena
10	některé soubory nemohly být zkontrolovány (mohou obsahovat hrozby)
50	nalezena hrozba
100	chyba

Návratové hodnoty větší než 100 znamenají, že soubor nebyl zkontrolován a může být infikován.

Řešení nejčastějších problémů

Tato kapitola obsahuje některé z nejčastěji se vyskytujících otázek a problémů, se kterými se můžete setkat. Klikněte na název kapitoly pro zobrazení řešení problému.

- Jak aktualizovat ESET Endpoint Security?
- Jak aktivovat ESET Endpoint Security?
- ESET Endpoint Security detekoval hrozbu
- Jak odstranit vir z počítače?
- Jak povolit komunikaci pro konkrétní aplikaci?
- Jak vytvořit novou úlohu v Plánovači?
- Jak naplánovat každý týden kontrolu počítače?
- Jak spravovat oznámení a interaktivní upozornění?
- Jak připojit PRODUCTNAME k ESET PROTECT?
  - Jak dočasně změnit nastavení vynucené politikou?
  - Jak aplikovat doporučené politiky pro ESET Endpoint Security
- Jak vytvořit mirror?
- Jak přejít na Windows 10 s nainstalovaným ESET Endpoint Security?
- Jak aktivovat vzdálené monitorování a správu produktu (RMM)?
- Jak zablokovat stahování konkrétních typů souborů z internetu
- Jak minimalizovat uživatelské rozhraní ESET Endpoint Security?

Pokud není váš problém uveden v seznamu výše, zkuste v nápovědě k produktu ESET Endpoint Security vyhledat řešení podle klíčového slova nebo fráze, která popisuje váš problém.

Pokud nenaleznete řešení vašeho problému v nápovědě, navštivte pravidelně aktualizovanou ESET Databázi znalostí. Níže naleznete odkazy na nejnavštěvovanější články v databázi.

- Jak odinstalovat ESET Endpoint Security
- Doporučení pro boj proti Filecoderu (ransomware)
- FAQ: ESET Endpoint Security a ESET Endpoint Antivirus
- Jaké adresy a porty povolit ve firewallu pro zajištění plné funkčnosti produktu ESET?

Pokud je to nutné, můžete se obrátit přímo na naše pracovníky technické podpory. Kontaktní formulář naleznete přímo v hlavním okně programu na záložce **Nápověda a podpora**.

Nejčastější dotazy týkající se automatické aktualizace produktů

Další informace týkající se aktualizace produktu ESET Endpoint Security naleznete v následujících článcích v naší Databázi znalostí:
- Jaké typy produktových aktualizací ESET vydává?

Dojde k automatickému aktualizování počítače? Aktualizace je stažena před nebo po jeho restartování?

Ke stažení dojde před restartem, což znamená, že v této fázi dojde k připravení aktualizovaných souborů. Po restartování jsou aktualizované soubory stále pouze připraveny k použití a aktuálně nainstalovaná verze poskytuje nepřetržitou ochranu. Změny se projeví po dalším spuštění produktu z řady ESET Endpoint Security.

Předpokládejme, že mám v síti přibližně 3000 počítačů. Dojde k souběžnému aktualizování všech počítačů? Mohu pro automatickou aktualizaci takového množství počítačů využít proxy?

Ve větších sítích můžete využít ESET Bridge, Mirror Tool, stejně tak proxy řešení, kdy se aktualizace z internetu stáhne pouze jednou a následně je distribuována lokálně. Aktualizace jsou menší, obvykle mají 5-10 MB, a v prvních týdnech od vydání jsou distribuovány postupně. Z tohoto důvodu si klienti, kteří se připojují přímo k serverům ESET, nezačnou stahovat aktualizace současně.

Mohu se rozhodnout kolik, nebo které počítače se mají automaticky aktualizovat? Nechci stahovat aktualizace pro více než deset počítačů za hodinu, případně chci deset počítačů aktualizovat právě teď, a další počítače až v dalších dnech.

Ve spravovaných prostředích je možné automatické aktualizace řídit pomocí politiky, ve které lze definovat nejvyšší požadovanou verzi. Podporovány jsou také zástupné znaky (například 9.0.2032.*). Další informace naleznete v online nápovědě k ESET PROTECT Cloud, resp. ESET PROTECT. Aktuálně však není možné jiným způsobem omezit automatické aktualizace. Jednotlivým skupinám počítačů můžete přiřazovat více politik.

Konfigurují se automatické aktualizace výhradně prostřednictvím politik? Pokud nechci produkt ESET aktualizovat, stačí politiku deaktivovat?

Pokud je pro produkt z řady ESET Endpoint k dispozici hotfix zajišťující bezpečnost a stabilitu, produkt se aktualizuje i přesto, že jsou automatické aktualizace zakázány, a to dle podmínek stanovených v příslušném licenčním ujednáním s koncovým uživatelem (EULA). Společnost ESET využívá hotfixy zajišťující bezpečnost a stabilitu za účelem řešení kritických problémů a zajištění maximální bezpečnosti a stability vámi používaného produktu.

Politiku pro automatickou aktualizaci můžete přiřadit libovolné skupině počítačů bez ohledu na jejich aktuální konfiguraci automatických aktualizací. V nespravovaných prostředích může uživatel konfigurovat automatické aktualizace lokálně v rozšířeném nastavení produktu ESET.

Co když v politice definuji nejstarší dostupnou verzi? Dojde i přesto k aktualizování produktu?

Hotfixy a kritické hotfixy (aktualizace zajišťující bezpečnost a stabilitu) patří do mírně odlišné kategorie aktualizací. Pravidelné hotfixy patří mezi automatické aktualizace se standardní prioritou a bere se v potaz uživatelské nastavení. Kritické hotfixy mají nejvyšší prioritu, a proto se aplikují bez ohledu na nastavení definované uživatelem.

Jak budou fungovat aktualizace v offline prostředích? Může se k tomu použít offline repozitář?

V offline repozitáři se nachází též .dup a .fup soubory. Tato část repozitáře musí být stažena prostřednictvím nástrojem Mirror Tool, nikoli produktem s aktivní funkcí mirror. Další informace naleznete v kapitole Offline Repository - Windows v online nápovědě pro ESET PROTECT.

Jak produkty ESET zjistí, že je vyžadována jejich aktualizace? Z repozitáře? Odesílají se data na servery? V případě, že společnost ESET plánuje provést aktualizaci měsíc po vydání nové verze, a to platí pro celý svět, jsou na to servery ESET připraveny?

Produkty ESET si stahují automatické aktualizace z repozitáře. Servery jsou na to připraveny, protože tyto kritické aktualizace mají jen několik kB. Na kritické aktualizace se na serverech repozitáře neuplatňují žádná omezení (throttling). Pokud by byly automatické aktualizace větší, můžeme omezení na serverech uplatit. V níže uvedené tabulce uvádíme příklad velikostí hotfixů v případě rozdílové automatické aktualizace:

Předchozí verze	Nová verze	Velikost
9.0.2032.2	9.0.2032.6	420 kB
8.1.2037.2	9.0.2032.2	6,5 MB
8.0.2028.0	9.0.2032.2	11,5 MB

V případě, že by došlo k selhání přírůstkové automatické aktualizace, produkt ESET může inicializovat stažení úplné aktualizace. Stále se jedná o automatickou aktualizaci se zárukou funkčnosti, místo .dup souboru se však stáhne větší soubor .fup. V případě verze 9.0.2032.2 je to 27 MB. Takový scénář je však ojedinělý.

Je při uvolňování automatické aktualizace pro ESET Endpoint Security uplatňováno nějaké omezení? Pokud ano, jak dlouho je omezení po aktualizaci platné?

Omezení se uplatňuje v průběhu prvních týdnů od vydání nové verze za účelem snížení zátěže na naše servery a zajištění rovnoměrné distribuce nové verze.

Domnívám se, že se automatické aktualizace budou jednou patřit mezi z hlavní způsoby, jak přejít na novou verzi. Jak to funguje podrobně?

Našim cílem je zajistit, aby se co nejvíce produktů u zákazníků aktualizovalo prostřednictvím automatických aktualizací. Udržovat podporu mnoha starých verzí je velmi obtížné. Funkce zajišťující automatické aktualizace produktů funguje jednoduše. Soubory .dup se stáhnou při první kontrole dostupnosti modulů. V průběhu aktualizace je produkt plně funkční a stále zajišťuje ochranu počítače. Nová verze se aktivuje po restartování počítače. Ve spravovaných prostředích můžete prostřednictvím politiky (například v ESET PROTECT) definovat nejvyšší možnou verzi, na kterou se mohou produkty aktualizovat, případně použít zástupné znaky. Další informace naleznete v online nápovědě k ESET PROTECT Cloud, resp. ESET PROTECT.

Je pravda, že automatické aktualizace fungují na 1/10? Nyní používám ESET Endpoint Security ve verzi 8.0.2028.1. Pokud je povolena automatická aktualizace, na jakou verzi se produkt aktualizuje?

Aktualizace produktů prostřednictvím automatických aktualizací může být opožděna z důvodu aktivovaných omezení na serverech repozitáře. Pokud je při vydání aktualizace produktu aktivní throttling, produkt si ji nemusí při pravidelné kontrole dostupnosti automatické aktualizace stáhnout okamžitě. V případě, že je aktualizace považována za bezpečnou a stabilní, může být omezení následně upraveno nebo zcela zrušeno, aby aktualizace byla doručena všech zbývajícím klientům.

Omezování (throttling) je proces, ve kterém se uplatňuje sada opatření, a může být pro každou aktualizaci platný různou dobu. Tato doba závisí na množství klientů, kteří si aktualizaci žádají, stejně tak zatížení našich serverů a dalších faktorech. Tento postup se neustále vyvíjí a mění.

Pokud spustím počítač v 8:45 a následně jej 17:00 vypnu, kdy dojde k automatické aktualizaci?

K automatické aktualizaci dojde s další úspěšnou naplánovanou aktualizací modulů, a to nejvýše jednou za 24 hodin.

Pokud v průběhu automatické aktualizace dojde k vypnutí počítače, kdy se provede další aktualizace?

Aktualizace se spustí v příštím naplánovaném aktualizačním okně. Postup automatické aktualizace (dříve známý jako uPCU) je postaven na robustním bezpečnostním mechanismu. Po stažení aktualizace a restartování počítače jsou aktualizované soubory stále pouze připraveny k použití a aktuálně nainstalovaná verze poskytuje nepřetržitou ochranu. Změny se projeví po dalším spuštění produktu z řady ESET Endpoint.

Jak mohu spustit automatické aktualizace okamžitě bez čekání na pravidelné spojení jednou za 24 hodin? Existuje nějaký jiný způsob, než kliknutí na tlačítko Zkontrolovat aktualizace?

Automatickou aktualizaci lze vyvolat ručně pouze kliknutím v hlavním okně programu v nabídce **Aktualizace** > na tlačítko **Zkontrolovat aktualizace**. Všechny ostatní způsoby pro aktualizací modulů se řídí politikou plánovače 24hodinových automatických aktualizací. V současné době není možné vzdáleně inicializovat stažení

automatických aktualizací. Tuto funkci plánujeme přidat v některé z dalších verzí.

Jak aktualizovat ESET Endpoint Security?

Aktualizaci produktu ESET Endpoint Security můžete provádět ručně nebo automaticky. Pro zahájení aktualizace přejděte v hlavním okně programu na záložku **Aktualizace** a klikněte na možnost **Zkontrolovat aktualizace**.

Po nainstalování programu se standardně vytvoří naplánovaná úloha, která spouští automatickou aktualizaci každou hodinu. Pokud chcete změnit tento interval, přejděte na záložku **Nástroje** > Plánovač.

Jak odstranit vir z počítače?

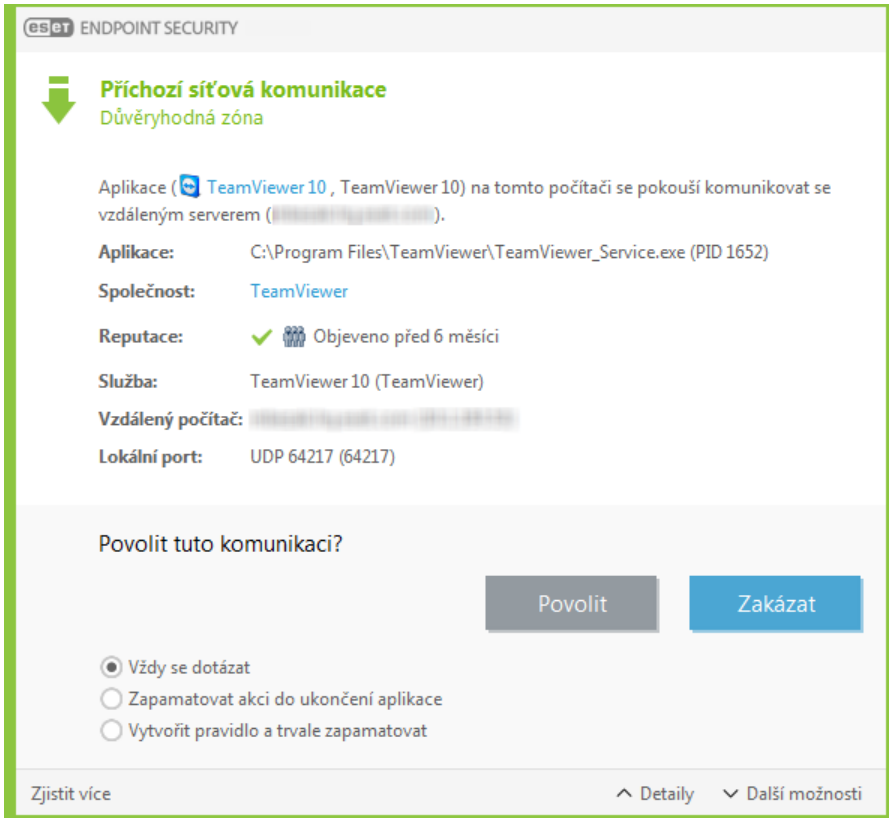
Pokud jeví počítač známky infekce, tzn. je pomalejší, zamrzá apod. doporučujeme postupovat podle následujících kroků:

1. V hlavním okně programu klikněte na záložku **Kontrola počítače**.
2. Klikněte na možnost **Smart kontrola** pro zahájení kontroly počítače,
3. Po dokončení kontroly si zobrazte její protokol. Zaměřte se především na počet zkontrolovaných, infikovaných a vyléčených souborů.
4. Pokud chcete zkontrolovat pouze určité části počítače, vyberte možnost **Volitelná kontrola** a ručně vyberte cíle kontroly.

Pro podrobnější informace navštivte pravidelně aktualizovanou ESET Databázi znalostí (článek nemusí být dostupný ve všech jazycích).

Jak povolit komunikaci pro konkrétní aplikaci?

Pokud je detekováno nové spojení/komunikace v interaktivním režimu firewallu, pro kterou ještě nebylo vytvořeno pravidlo, zobrazí se dialogové okno, ve kterém můžete komunikaci povolit nebo zakázat. Pokud chcete, aby ESET Endpoint Security provedl vybranou akci při každém pokusu o komunikaci, zaškrtněte možnost **Zapamatovat akci (vytvořit pravidlo)**.



Pro aplikace, které dosud firewall produktu ESET Endpoint Security nedetekoval, můžete vytvořit nové pravidlo. Editor pravidel si otevřete kliknutím v hlavním menu na záložku **Nastavení** > **Síť**, kde klikněte na ozubené kolečko na řádku **Firewall** a ze zobrazeného kontextového menu vyberte možnost **Nastavit**. V zobrazeném rozšířeném nastavení přejděte na záložku **Rozšířené** a klikněte na **Změnit** na řádku **Pravidla**.

Pro vytvoření pravidla klikněte na tlačítko **Přidat**. Klikněte na tlačítko Přidat a na záložce **Obecné** zadejte název pravidla, směr a komunikační protokol pro nové pravidlo. V tomto okně můžete definovat akci, která se provede při aplikaci daného pravidla.

Na záložce **Lokální strana** vyberte aplikaci na tomto počítači, která komunikuje a definujte port. Na záložce **Vzdálená strana** zadejte vzdálenou adresu a port (pokud je to potřeba). Nově vytvořené pravidlo se aplikuje ihned po detekci dané komunikace.

Jak vytvořit novou úlohu v Plánovači?

Pro vytvoření nové úlohy v Plánovači přejděte v hlavním okně programu na záložku **Nástroje** > **Plánovač** a klikněte na tlačítko **Přidat** v dolní části okna nebo z kontextového menu dostupného po kliknutím pravým tlačítkem myši vyberte možnost **Přidat**. K dispozici jsou následující typy úloh:

- **Spuštění externí aplikace** – vyberte si aplikaci, kterou chcete pomocí plánovače spustit.
- **Údržba protokolů** – v protokolech mohou přirozeně zůstat zbytky po již smazaných záznamech. Tato úloha zajistí optimalizaci záznamů v protokolech, což zajistí efektivnější a rychlejší práci s nimi.
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému.
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě.
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači,
- **Aktualizace** – zajišťuje aktualizaci detekčních a programových modulů.

Mezi nejčastěji používané naplánované úlohy patří **Aktualizace**, proto si podrobněji popíšeme přidání nové aktualizační úlohy.

V rozbalovacím menu **naplánovaná úloha** vyberte možnost **Aktualizace**. Zadejte **Název úlohy** a klikněte na tlačítko **Další**. Dále nastavte pravidelnost opakování úlohy. K dispozici jsou následující možnosti: **Jednou**, **Opakovaně**, **Denně**, **Týdně**, **Při události. Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii nebo počítače z UPS, zapněte možnost Nespouštět úlohu, pokud je počítač napájen z baterie**. Po kliknutí na tlačítko Další zadejte čas **Provedení úlohy**. Dále je potřeba definovat akci, která se provede v případě, že ve stanoveném termínu nebude možné úlohu spustit. K dispozici jsou následující možnosti:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

V dalším kroku se zobrazí souhrnné informace o přidávané naplánované úloze. Akci dokončete kliknutím na tlačítko **Dokončit.**

Následně se zobrazí dialogové okno. V něm vyberte profil, který se použije pro naplánovanou úlohu. Nastavte primární a sekundární profil. Sekundární profil se použije v případě, kdy nebude možné provést úlohu pomocí primárního profilu. Kliknutím na tlačítko **Dokončit** se vytvořená naplánovaná úloha přidá do seznamu naplánovaných úloh.

Jak naplánovat každý týden kontrolu počítače?

Pro naplánování standardní úlohy otevřete hlavní okno programu > **Nástroje** > **Plánovač**. Níže je popsán stručný návod, jak vytvořit úlohu, která bude kontrolovat lokální disky každých týden. Přečtěte si detailní postup v naší Databázi znalostí.

Pro naplánovaní úlohy postupujte následovně:

1. Klikněte na tlačítko **Přidat** v hlavním okně Plánovače.
2. V rozbalovacím menu vyberte možnost **Volitelná kontrola počítače**.
3. Zadejte název úlohy a klikněte na možnost **Týdně**.
4. Vyberte datum a čas, kdy chcete úlohu spustit.
5. Vyberte akci, která se provede v případě neprovedení úlohy ve stanoveném čase (například **Jakmile je to možné**). Tím zajistíte spuštění úlohy, pokud byl počítač vypnutý.
6. Zkontrolujte všechna nastavení úlohy v seznamu a klikněte na **Dokončit**.
7. V rozbalovacím menu **Cíle kontroly** vyberte **Lokální disky**.
8. Kliknutím na tlačítko **Dokončit** potvrdíte její naplánování.

Jak připojit ESET Endpoint Security k ESET PROTECT?

Pokud jste do počítače nainstalovali ESET Endpoint Security a chcete se připojit prostřednictvím ESET PROTECT, ujistěte se, že máte na klientské pracovní stanici nainstalovaného také ESET Management Agenta. Jedná se o nezbytnou součást pro komunikaci klienta s ESET PROTECT Serverem.

- Instalace nebo nasazení ESET Management Agenta

Další informace:

- Příručka pro vzdáleně spravované produkty
- Jak dočasně změnit nastavení vynucené politikou?
- Jak aplikovat doporučené politiky pro ESET Endpoint Security

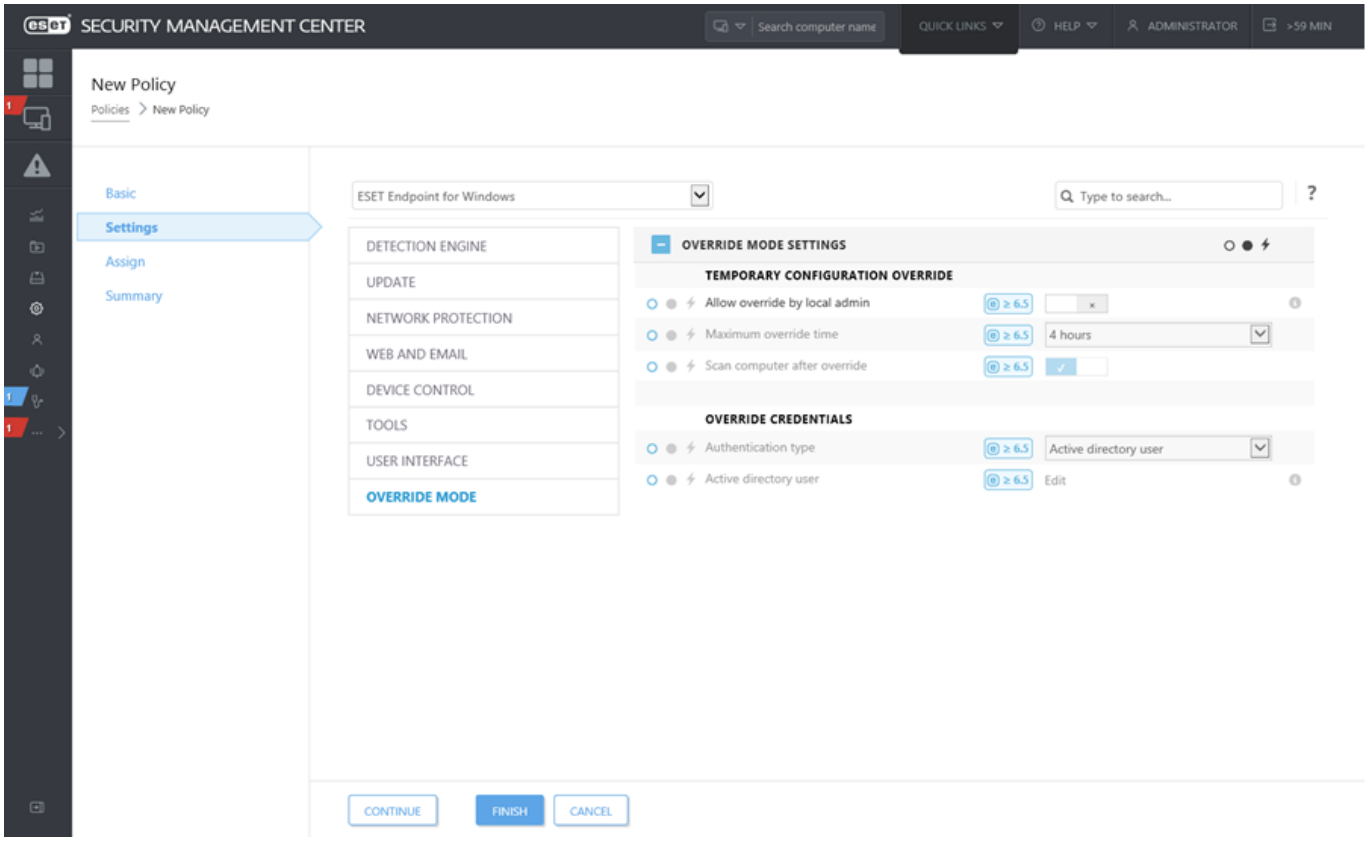
Jak dočasně změnit nastavení vynucené politikou?

Uživatelům používajícím na Windows produkty z řady ESET Endpoint ve verzi 6.5 a novější můžete dočasně umožnit změnu nastavení, které je jinak vynucenou politiku, a není možné jej lokálně měnit. Prostřednictvím režimu dočasné změny nastavení umožníte lokálním administrátorům měnit konfiguraci bezpečnostního produktu ESET, která je jinak aplikována politikami. Dočasně měnit nastavení mohou vámi definovaní uživatelé z Active Directory, případně všichni uživatelé za předpokladu, že znají heslo. Tato funkce může být aktivní nejvýše po dobu čtyř hodin.

⚠ Režim dočasné změny nastavení nelze vzdáleně z ESET PROTECT Web Console ukončit, pokud je spuštěn. Vypne se automaticky po uplynutí stanového intervalu. Případně jej uživatel může deaktivovat ručně. Uživatel, který použije režim dočasné změny nastavení musí mít rovněž oprávnění administrátora Windows. V opačném případě nebude schopen uložit změny v nastavení produktu ESET Endpoint Security. Skupina uživatelů Active Directory je podporována.

Pro povolení **dočasné změny nastavení** na konkrétní stanici:

1. V hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.
2. V sekci **Obecné** zadejte **název** politiky, volitelně **popis**.
3. V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows**.
4. V konfigurační šabloně přejděte na záložku **Dočasná změna nastavení**.
5. V sekci **Přiřadit** vyberte konkrétní stanici nebo skupinu zařízení, na které chcete politiku uplatnit.
6. Souhrnné informace naleznete v sekci **Přehled** a politiku uložte kliknutím na tlačítko **Dokončit**.



Uživatel *Filip* měl problém s přístupem na konkrétní webovou stránku. Administrátor se rozhodl, že umožní Filipovi dočasně měnit nastavení, aby mohl svépomocí identifikovat příčinu. Administrátor si následně jeho konfiguraci vzdáleně stáhl do ESET PROTECT a převedl do politiky.
Administrátor k tomu využil tento postup:
1. V hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.
2. Zadejte **název** nové politiky, volitelně **popis**. V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows**.
3. V konfigurační šabloně přejděte na záložku **Dočasná změna nastavení**. Pomocí přepínače tuto možnost aktivujte, nastavte limit na 1 hodinu a vyberte konkrétního *uživatele* z Active Directory.
4. Přiřaďte politiku požadované stanici (v našem případě *počítači Filipa*) a klikněte na tlačítko **Dokončit** pro uložení politiky.
5. Uživatel *Filip* má nyní v rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu možnost pro dočasnou změnu nastavení a může měnit konfiguraci programu.
6. V ESET PROTECT Web Console na záložce **Počítače** najděte konkrétní stanici (v našem případě *Filipa*) a klikněte na možnost **Zobrazit detaily**.
7. Přejděte na záložku **Konfigurace** a klikněte na tlačítko **Vyžádat konfiguraci**.
8. Vyčkejte na zobrazení konfigurace. Klikněte na konfiguraci požadovaného produktu a z kontextového menu vyberte možnost **Otevřít konfiguraci**.
9. Zkontrolujte nastavení a klikněte na tlačítko **Převést do politiky**.
10. Zadejte **název** nové politiky, volitelně **popis**.
11. V sekci **Nastavení** zkontrolujte konfiguraci a případně ji ještě upravte.
12. **Přiřaďte** politiku požadované stanici (v našem případě *Filipovi*).
13. Pro uložení klikněte na tlačítko **Dokončit**.
14. Nezapomeňte stanici odebrat politiku dočasné změny nastavení produktu, pokud není používána.

Jak aplikovat doporučené politiky pro ESET Endpoint

Security

Po připojení ESET Endpoint Security k ESET PROTECT doporučujeme na stanici aplikovat politiku – ať již některou z doporučených nebo vámi vytvořenou.

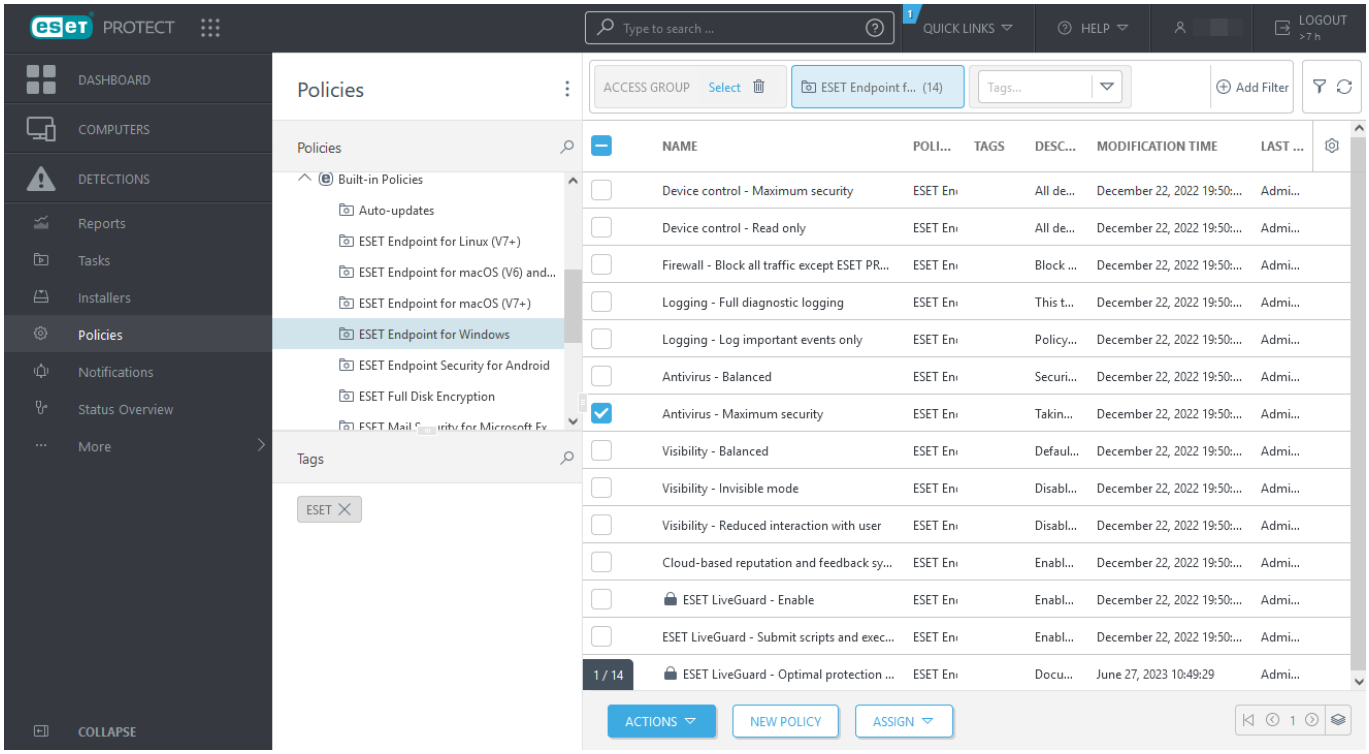
K dispozici je několik předdefinovaných politik pro ESET Endpoint Security:

Politika	Popis
Antivirus – Vyvážené nastavení	Bezpečnostní konfigurace doporučená pro většinu situací.
Antivirus – Maximální zabezpečení	Aktivuje se strojové učení, rozšířená heuristika, hloubková analýza chování a filtrování protokolu SSL. Tyto funkce mají vliv na detekci potenciálně zneužitelných, nechtěných a podezřelých aplikací.
Cloudový systém reputace a zpětné vazby	Aktivuje zapojení do cloudového reputačního systému ESET LiveGrid®, který vylepší detekci zcela nových hrozeb a sdílením škodlivých vzorků a potenciálních hrozeb pomůžete vylepšit detekční schopnosti.
Správa zařízení – Maximální zabezpečení	Všechna zařízení budou blokována. Připojení jakéhokoli zařízení k počítači bude muset povolit administrátor.
Správa zařízení – režim pro čtení	Z připojených zařízení bude možné pouze data číst. Zápis nebude povolen.
Firewall – Blokovat veškerou komunikaci kromě ESET PROTECT a ESET Inspect	Zablokuje veškerou síťovou komunikaci a povolí pouze spojení s ESET PROTECT a ESET Inspect serverem (pouze pro ESET Endpoint Security).
Protokolování – Aktivovat diagnostické protokolování	Do protokolů se budou zaznamenávat všechny události a sbírat se začnou všechny protokoly, včetně modulu HIPS a parametrů skenovacího jádra ThreatSense. Bude zaznamenáno vše, co překračuje minimální nastavenou úroveň. Protokoly budou automaticky odstraněny po 90 dnech.
Protokolování – Zaznamenávat pouze důležité události	Zaznamenávány budou pouze varování, chyby a kritické události. Protokoly budou automaticky odstraněny po 90 dnech.
Viditelnost – Vyvážené nastavení	Výchozí nastavení. Zobrazovat se budou oznámení i stavy aplikace.
Viditelnost – Neviditelný režim	Deaktivuje zobrazování oznámení, grafické uživatelské rozhraní a integraci do kontextového menu. Nepoběží proces egui.exe. Vhodné pro kompletní správu prostřednictvím ESET PROTECT Cloud.
Viditelnost – Nižší míra interakce s uživatelem	Deaktivuje zobrazování oznámení a stavů aplikace, ale grafické uživatelské rozhraní poběží.

Pro aplikování politiky s názvem **Antivirus – Maximální zabezpečení**, která definuje více než 50 doporučených nastavení pro produkt ESET Endpoint Security, postupujte podle níže uvedených kroků:

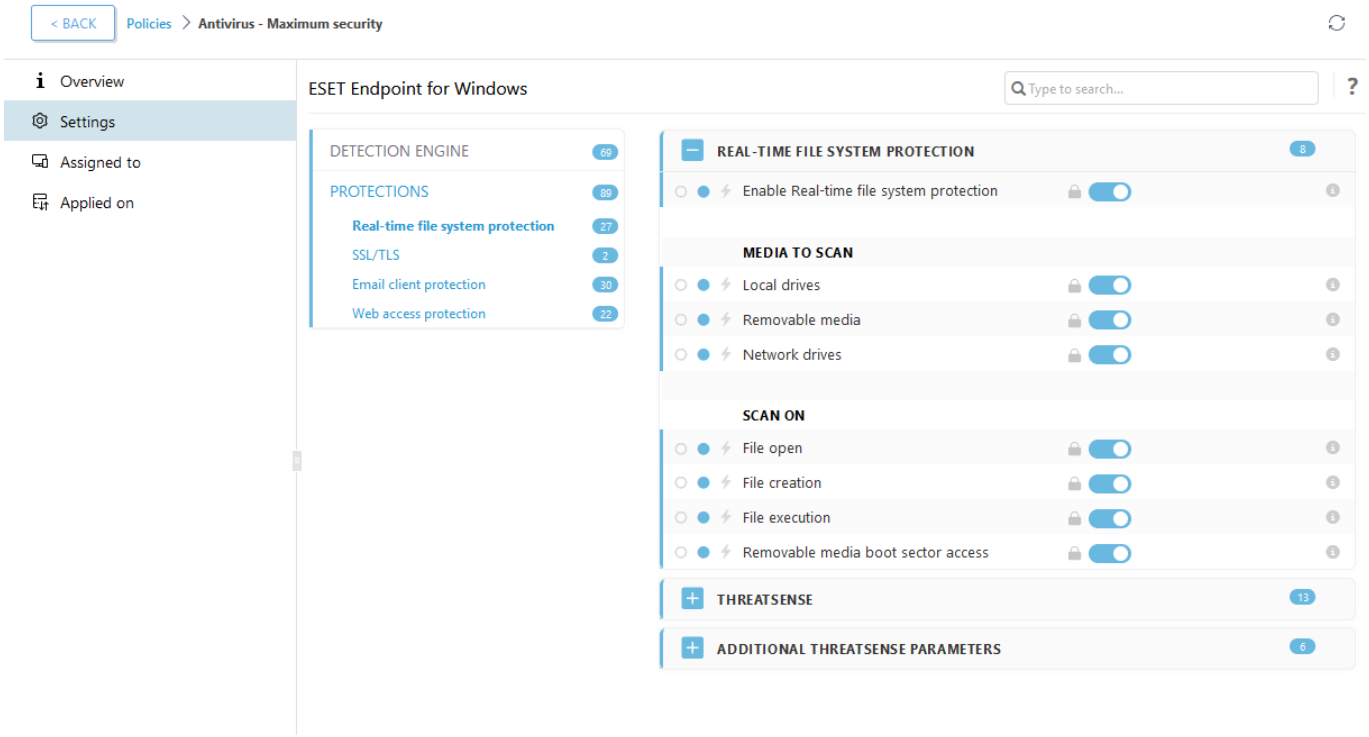
> Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:
> Aplikování doporučeného nastavení nebo předdefinované politiky pro ESET Endpoint Security prostřednictvím ESET PROTECT

1. Otevřete si ESET PROTECT Web Console
2. V hlavním menu přejděte na záložku **Politiky** a rozbalte položku **Předdefinované politiky** > **ESET Endpoint for Windows**.
3. Klikněte na položku **Antivirus – Maximální zabezpečení – Doporučeno**.
4. Na záložce **Přiřazeno k** klikněte na tlačítko **Přiřadit klientovi** nebo **Přiřadit skupině** a vyberte cíl, na který chcete politiku aplikovat.



Pro zobrazení konfigurace, kterou touto politikou aplikujete přejděte na záložku **Nastavení**.

- Modrá tečka představuje nastavení definované v této politice
- Číslo v modrém bublině představuje počet nastavení definované v dané sekci touto poltiikou
- Více informací o ESET PROTECT politikách



Jak vytvořit mirror?

ESET Endpoint Security dokáže vytvářet kopie aktualizací (detekčního jádra a dalších modulů), z níž lze pak aktualizovat další stanice v lokální síti, na kterých je nainstalován například ESET Endpoint Antivirus nebo ESET Endpoint Security.

Aktualizační mirror produktu ESET Endpoint Security vytváří kopie aktualizací pouze pro stejnou generaci produktu na platformě Windows- Příklad: z mirroru vytvořeného produktem ESET Endpoint Security pro Windows ve verzi 10.x je možné aktualizovat pouze ESET Endpoint Antivirusa ESET Endpoint Security pro Windows ve verzi 10.x.

Zpřístupnění aktualizačního mirroru prostřednictvím interního HTTP serveru poskytovaného produktem ESET Endpoint Security

1. V hlavním okně programu stiskněte klávesu **F5** a otevřete si **Rozšířená nastavení**. Přejděte do sekce **Aktualizace** > **Profily**.
2. Rozbalte záložku **Aktualizace** a v sekci **Aktualizace modulů** se ujistěte se, že máte aktivní možnost **Automatický výběr serveru**.
3. Rozbalte záložku **Aktualizační mirror** a aktivujte zde možnost **Vytvářet kopie aktualizací** a **Zapnout HTTP server**.

Další informace naleznete v následujících kapitolách:
- Aktualizační mirror
- Aktualizace z mirroru

Zpřístupnění aktualizačního mirroru prostřednictvím síťového sdílení

1. Nejprve je nutné na lokálním nebo síťovém zařízení vytvořit sdílenou složku. Při jejím vytváření musíte nastavit práva pro zápis do této složky uživateli, který bude kopie aktualizací do této složky ukládat (lokální účet SYSTEM), a nastavit práva pro čtení uživatelům, kteří si aktualizace z této složky budou stahovat (tedy všem uživatelům, kteří používají bezpečnostní produkt ESET).
2. Dále v **Rozšířeném nastavení** v sekci **Aktualizace** >**Profily** > **Aktualizační mirror** aktivujte možnost **Vytvářet kopie aktualizací**.
3. Klikněte na **Vymazat** a následně na **Změnit** pro vybrání **složky**, do které chcete aktualizace ukládat. Najděte a vyberte vytvořenou sdílenou složku.

Pokud nechcete poskytovat aktualizace modulu prostřednictvím interního HTTP serveru, deaktivujte možnost **Zapnout HTTP server**.

Jak přejít na Windows 10 s nainstalovaným ESET Endpoint Security?

Před stažením a nainstalováním aktualizace na Windows 10 doporučujeme nejprve aktualizovat produkt ESET na nejnovější verzi a aktualizovat detekční a programové moduly. Tímto způsobem si zajistíte maximální ochranu v průběhu celého procesu aktualizace operačního systému a předejdete případným konfliktům při použití nepodporované verze.

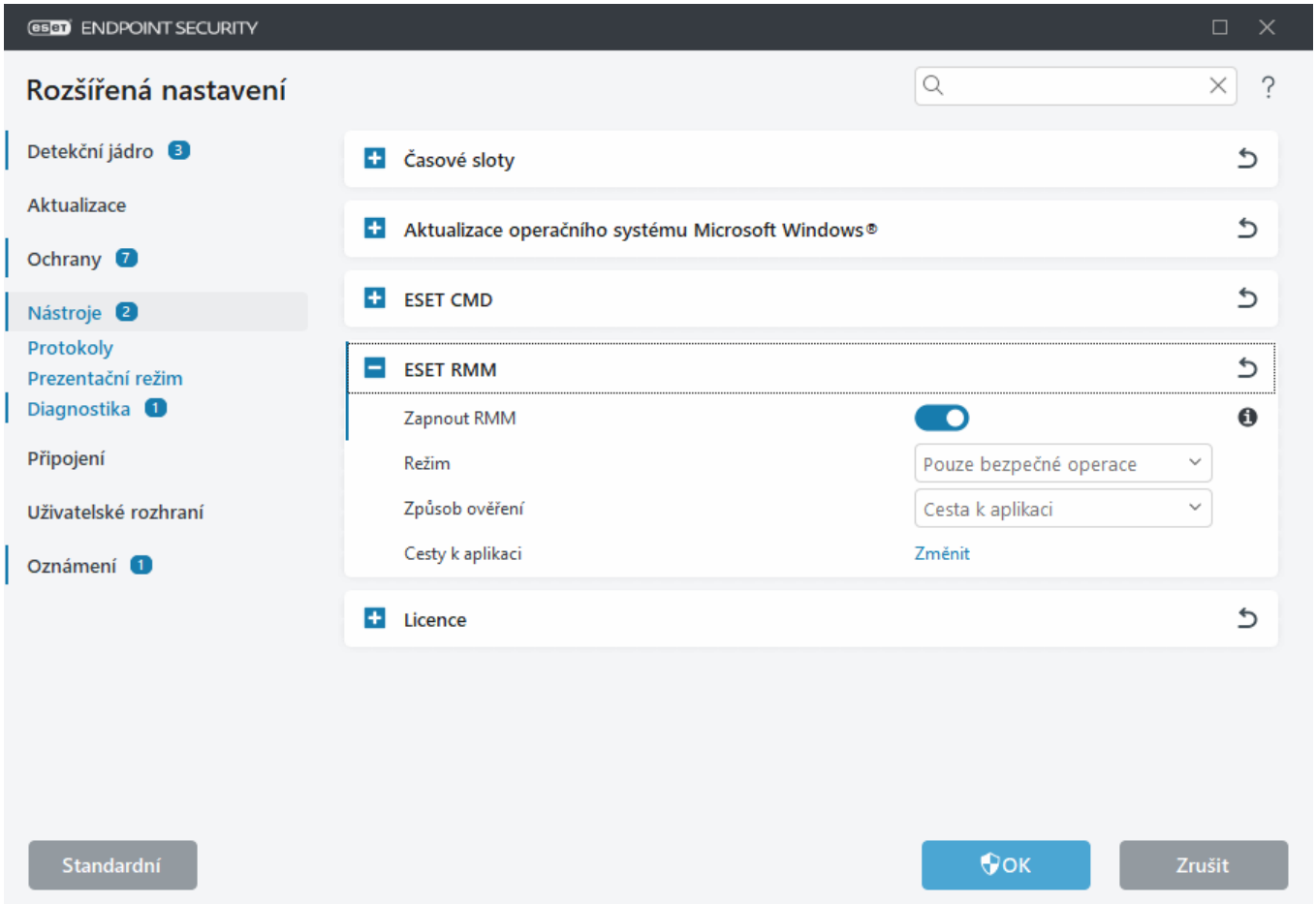
Další jazykové verze:

Pokud si potřebujete stáhnout instalační balíček v jiném jazyce, přejděte na webových stránkách společnosti ESET do sekce Stáhnout.

> Více informací o kompatibilitě produktů ESET s operačním systémem Windows 10 naleznete v ESET Databázi znalostí.

Jak aktivovat vzdálené monitorování a správu produktu (RMM)?

Remote Monitoring and Management (RMM) je způsob pro vzdálené monitorování a ovládání aplikací z jednoho místa (počítačů, serverů i mobilních zařízení) prostřednictvím agenta instalovaného na koncových stanicích. ESET Endpoint Security podporuje správu prostřednictvím nástrojů třetích stran od verze 6.6.2028.0.



Standardně je ESET RMM vypnutý. Pro aktivaci ESET RMM, otevřete Rozšířená nastavení > **Nástroje** > **ESET RMM** a klikněte na přepínač u položky **Zapnout RMM**.

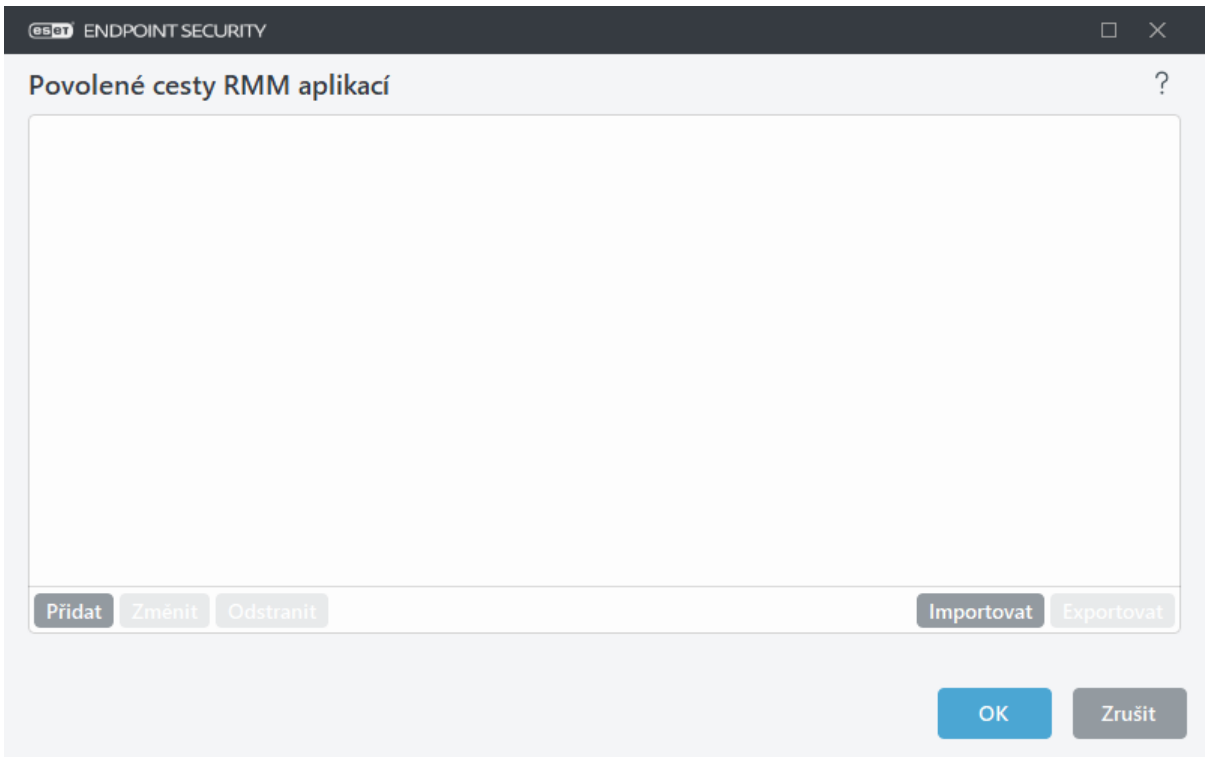
Režim – možnost **Pouze bezpečné operace** vyberte v případě, kdy RMM rozhraní chcete aktivovat pouze v režimu pro čtení a provádění bezpečných operací. Vybráním možnosti **Všechny operace** zajistíte provádění všech operací prostřednictvím RMM.

Operace	Režim: pouze bezpečné operace	Režim: všechny operace
Získání informací o aplikaci	✔	✔
Získání konfigurace	✔	✔
Získání informace o licenci	✔	✔
Získání protokolů	✔	✔
Získání stavu ochrany	✔	✔
Získání stavu aktualizace	✔	✔
Získání konfigurace		✔
Spuštění aktivace		✔
Spuštění kontroly	✔	✔
Spuštění aktualizace	✔	✔

Způsob ověření – rozhodněte se, zda se RMM klient bude autorizovat. Pro aktivování vyberte možnost **Cesta k aplikaci** a níže definujte cestu k RMM klientovi.

Nástroj RMM by se měl vždy autorizovat, aby se zabránilo tomu, že jej produkt ESET vyhodnotí jako škodlivý kód, který se snaží deaktivovat nebo obejít ochranu produktu.

Cesty k aplikaci – pokud jste výše nastavili jako způsob ověření Cesta k aplikaci, klikněte na možnost Změnit pro zobrazení okna Povolené cesty RMM aplikací. Následně definujte povolené aplikace, které mohou RMM využívat.



Přidat – kliknutím přidáte cestu k RMM aplikaci. Cestu zadejte ručně nebo ji vyberte kliknutím na tlačítko **…**.

Změnit – po kliknutí můžete upravit existující záznam. To se může hodit v případě, kdy se **změnila** cesta k aplikaci.

Odstranit – kliknutím odstraníte záznam k povolené RMM aplikaci.

Soubor ermm.exe naleznete standardně ve složce s produktem ESET Endpoint Security (například C:*Program*

Files\ESET\ESET Security. Binárka ermm.exe zajišťuje výměnu dat s RMM doplňkem, který komunikuje s RMM agentem, jenž je spojen s RMM serverem.

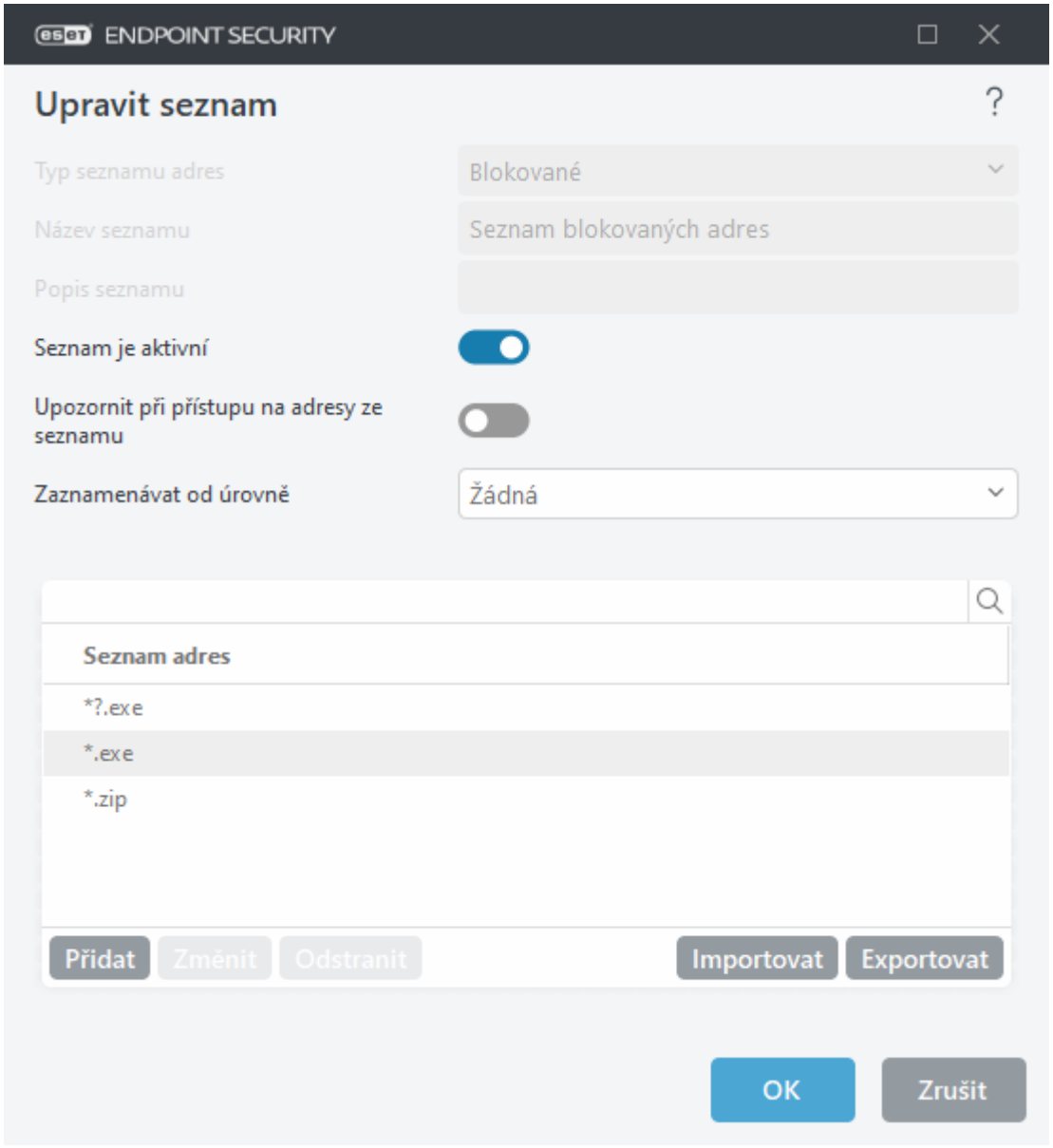
- ermm.exe – nástroj příkazového řádku vyvinutý společností ESET, který umožňuje správu firemních bezpečnostních produktů a komunikaci s RMM doplňkem.
- RMM Plugin je doplněk třetí strany, který běží lokálně na Windows stanici chráněné produktem ESET Endpoint. Tento doplněk komunikuje s konkrétním RMM Agentem (například Kaseya) a ermm.exe.
- RMM Agent je aplikace třetí strany (například Kaseya), která běží lokálně na Windows stanici chráněné produktem ESET Endpoint. Agent komunikuje s RMM doplňkem a RMM serverem.

Jak zablokovat stahování konkrétních typů souborů z internetu

Pro zakázání stahování konkrétních typů souborů (například .exe, .pdf nebo .zip) z internetu můžete využít součást pro správu URL adres a definovat masku souborů pomocí zástupných znaků. Stiskněte klávesu F5, čím se zobrazí **Rozšířená nastavení**. Přejděte do sekce **Web a mail** > **Ochrana přístupu na web** a rozbalte část **Správa URL adres**. Na řádku **Seznam adres** klikněte na **Změnit**.

V okně **Seznam adres** vyberte možnost **Seznam blokovaných adres** a kliknutím na tlačítko **Změnit** nebo **Přidat** vytvořte nebo upravte seznam. Otevře se nové dialogové okno. Pokud si chcete vytvořit nový seznam, jako typ seznamu vyberte **Blokované**, a seznam pojmenujte. Pokud chcete být upozorněni na přístup k nějaké adrese z aktuálního seznamu, klikněte na přepínač **Upozornit při přístupu na adresy ze seznamu**. Z rozbalovacího menu vyberte úroveň od které se má tento přístup **Zaznamenávat** do protokolu. ESET PROTECT může shromažďovat záznamy od úrovně **Varování**.

Možnosti nastavit úroveň pro zaznamenávání událostí do protokolu s hodnotou Informační a Varování je dostupná pouze v případě, kdy pravidlo obsahuje v rámci domény alespoň dvě komponenty bez zástupných znaků. Příklad:
- *.domain.com/*
- *www.domain.com/*



Klikněte na tlačítko **Přidat** a zadejte masku souboru, jehož stahování chcete blokovat. Pro zablokování konkrétního souboru z konkrétní webové stránky zadejte úplnou cestu k souboru, například *http://example.com/file.exe*. V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Otazník (?) představuje jeden proměnný znak, zatímco hvězdička (*) představuje řetězec proměnných složený z nula nebo více znaků. Maska **/*.zip* například blokuje stahování všech komprimovaných ZIP souborů.

Mějte na paměti, že prostřednictvím této možnosti můžete blokovat stahování konkrétních typů souborů pouze v případě, že je přípona uvedena v URL. Pokud je na webové stránce jako odkaz pro stažení použit například *www.example.com/download.php?fileid=42*, dojde ke stažení souboru bez ohledu na to, zda příponu blokujete.

Jak minimalizovat uživatelské rozhraní ESET Endpoint Security?

Při vzdálené správě stanice můžete využít předdefinovanou politiku s názvem Viditelnost.

Případně můžete kroky provést ručně:

1. V hlavním okně programu stiskněte klávesu **F5** a přejděte do Rozšířeného nastavení. Následně rozbalte

sekci **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

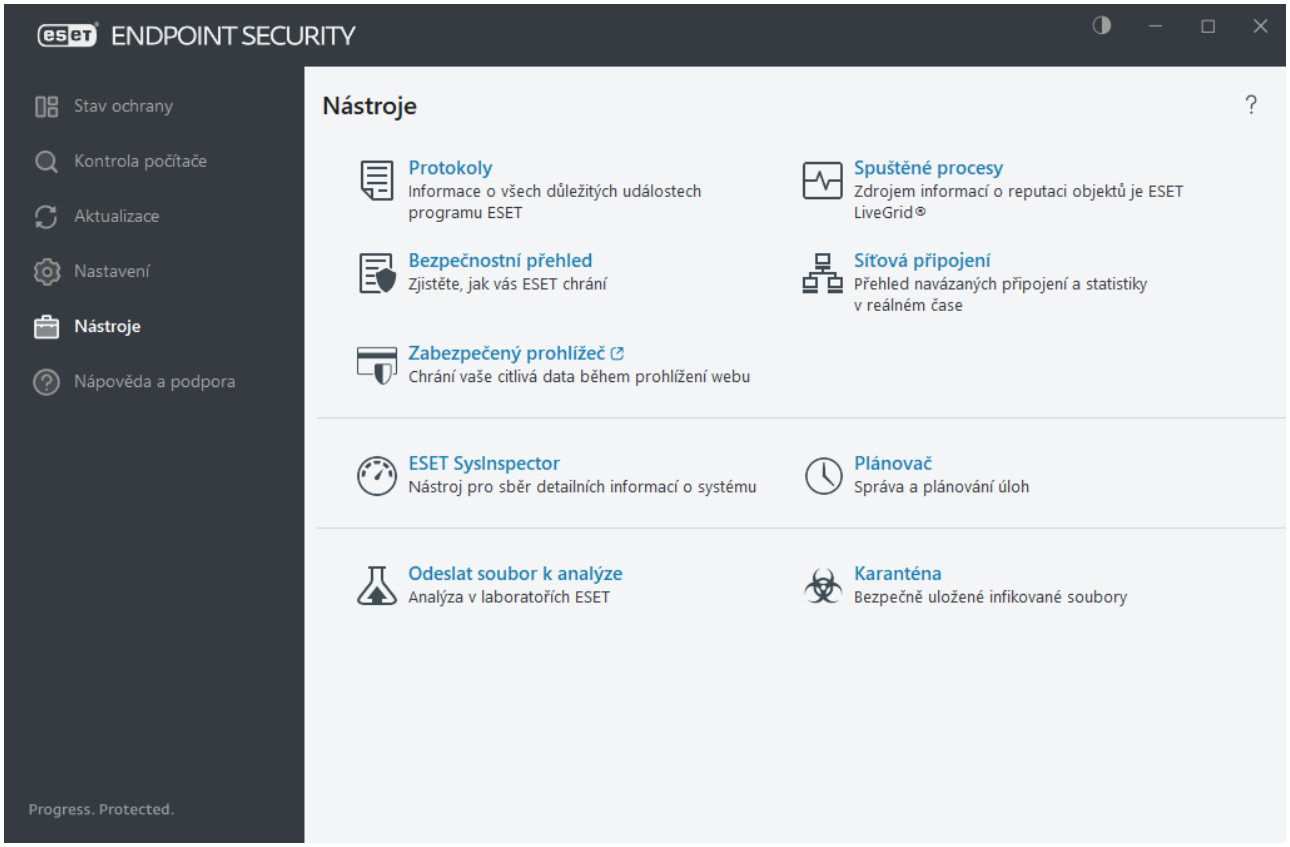
2. Vyberte si požadovaný **Režim spuštění** grafického rozhraní. Více informací o jednotlivých režimech naleznete v samostatné kapitole.
3. Deaktivujte možnost **Zobrazit úvodní obrázek při startu** a **Používat zvuková upozornění**.
4. Nastavte si Oznámení.
5. Nastavte si Stavy aplikace.
6. Nastavte si Potvrzovací zprávy.
7. Nastavte si Upozornění a informační okna.

Jak vyřešit situaci, kdy vás "Zabezpečený prohlížeč nepřesměroval na požadovanou webovou stránku"?

Pro vyřešení této situace postupujte podle níže uvedených kroků:

Po provedení každého kroku se ujistěte, zda Zabezpečený prohlížeč funguje.
Pokračujte dalšími kroky, až dokud se zabezpečený prohlížeč nespustí nebo nebude fungovat.

1. Restartujte svůj počítač.
2. Ujistěte, že používáte nejnovější verzi operačního systému Windows a firemního produktu ESET pro Windows: Jaká je nejnovější verze produktů pro firmy?



3. V některých případech může docházet ke konfliktu s bezpečnostními produkty nebo firewally třetích stran. Pro kontrolu konfliktů se soubory načtenými v prohlížeči si otevřete Protokoly > **Zabezpečený prohlížeč** a odinstalujte software třetích stran ve Windows v části Přidat nebo odebrat programy. V hlavním menu klikněte na **Nástroje** > **Zabezpečený prohlížeč**. Vyčkejte na otevření zabezpečeného prohlížeče a pokračujte dalším krokem.
4. Deaktivujte všechna rozšíření prohlížeče třetích stran.

5. Vymažte cache prohlížeče. Jak, smazat: cache u Mozilla Firefox, případně jak na cache v Google Chrome?
6. Ujistěte se, že prohlížeč označený v systému jako výchozí není v seznamu vyloučených aplikací. Otevřete Rozšířená nastavení > **Ochrany** > **Ochrana přístupu na web** > **Vyloučené aplikace**.
7. Pokud jste v předešlém kroku neinstalovali novou verzi produktu ESET, proveďte jeho opravnou instalaci. Následně restartujte počítač. Po restartu vypněte Zabezpečený prohlížeč a znovu zapněte. Následně zkuste spustit zabezpečený prohlížeč.

Zabezpečený prohlížeč představuje další vrstvu ochrany, která má chránit vaše finanční údaje během online transakcí.

Ve většině případů zabezpečený prohlížeč ochrání automaticky váš výchozí prohlížeč po návštěvě známé bankovní stránky. Chcete-li otevřít chráněný prohlížeč přímo, klikněte na **Nástroje** v ESET Endpoint Security a poté klikněte na  **Zabezpečený prohlížeč**.

Více informací o zabezpečeném prohlížeči naleznete v ESET Databázi znalostí:

- Jak používat ESET Zabezpečený prohlížeč?
- Jak zapnout nebo vypnout ESET Ochranu bankovnictví a online plateb
- Jak dočasně nebo trvale vypnout ESET Ochranu bankovnictví a online plateb
- Ochrana bankovnictví a online plateb – nejčastější chyby
- ESET Slovník pojmů | Ochrana bankovnictví a online plateb

Pokud se vám nedaří vyřešit potíže svépomocí, kontaktujte technickou podporu ESET.

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel”) Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční

klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro následující funkce Softwaru:

a) **Aktualizace Software**. Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace“), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti“, které jsou k dispozici na webu https://go.eset.com/eol_business. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

b) **Zasílání infiltrací a informací Poskytovateli.** Software obsahuje funkce, které slouží ke shromažďování vzorků počítačových virů a jiných škodlivých počítačových programů a podezřelých, problematických nebo potenciálně nežádoucích nebo nebezpečných objektů, jako jsou soubory, adresy URL, IP pakety a ethernetové rámce (dále jen "Infiltrace") a jejich následnému odeslání Poskytovateli, mimo jiné včetně informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, a informací o operacích a funkcích Softwaru ("Informace"). Informace a Infiltrace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) o Koncovém uživateli a/nebo jiných uživatelích počítače, na kterém je Software nainstalován, a soubory postižené Infiltracemi, včetně přidružených metadat.

Informace a Infiltrace mohou být shromažďovány následujícími funkcemi Softwaru:

i. Funkce Reputační systém LiveGrid zahrnuje shromažďování a odesílání jednosměrných hodnot hash, které souvisejí s Infiltracemi, Poskytovateli. Tato funkce je povolena v rámci standardního nastavení Softwaru.

ii. Funkce Systém zpětné vazby LiveGrid zahrnuje shromažďování a odesílání Infiltrací s příslušnými metadaty a Informacemi Poskytovateli. Tuto funkci aktivuje Koncový uživatel během procesu instalace Softwaru.

Poskytovatel bude obdržené Informace a Infiltrace používat pouze pro účely analýzy a zkoumání Infiltrací, zlepšování ověřování pravosti Softwaru a Licence a přijme veškerá vhodná opatření, aby zajistil, že obdržené Infiltrace a Informace zůstanou v bezpečí. Po aktivaci této funkce Softwaru mohou být Infiltrace a Informace shromažďovány a zpracovávány Poskytovatelem, jak je uvedeno v Zásadách ochrany osobních údajů a v příslušných právních předpisech. Tyto funkce můžete kdykoliv deaktivovat.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a

informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli

z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel

vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Zásady ochrany osobních údajů

Společnost ESET spol. s r.o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsaná v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. Abychom dosáhli tohoto cíle, zveřejňujeme zde tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků ("Koncový uživatel" nebo "Vy") o následujících tématech:

- Zpracování osobních údajů
- Důvěrnost údajů,
- Práva subjektu údajů.

Zpracování osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v Licenčním ujednáním s koncovým uživatelem ("EULA"), ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané ve smlouvě EULA a dokumentaci k produktu, například služby aktualizace/upgradu, ESET LiveGrid®, ochranu proti zneužití dat, podporu atd. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Aktualizace a další statistiky zahrnující informace o procesu instalace a vašem počítači, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako je operační systém, údaje o hardwaru, ID instalace, ID licencí, IP adresa, MAC adresa a nastavení konfigurace produktu.
- Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jako součást reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu.
- Podezřelé vzorky a metadata jako součást systému zpětné vazby ESET LiveGrid®, který umožňuje společnosti ESET okamžitě reagovat na potřeby našich koncových uživatelů a udržet akceschopnost tváří v tvář nejnovějším

hrozbám. Jsme závislí na tom, že nám zasíláte:

- infiltrace, jako jsou potenciální vzorky virů a jiných škodlivých programů, a podezřelé; problematické, potenciálně nežádoucí nebo nebezpečné objekty, jako jsou spustitelné soubory nebo e-mailové zprávy, které jsou nahlášeny koncovým uživatelem jako nevyžádané nebo označené naším produktem; údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- údaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
- Nemáme v úmyslu, aby byly součástí našich systémů nebo aby byly zpracovány pro účely uvedené v těchto Zásadách ochrany osobních údajů.

Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb. Kontaktní informace a údaje obsažené ve vašich požadavcích na podporu mohou být vyžadovány za účelem poskytování podpory. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory.

- Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory. Funkcí Ochrana proti zneužití dat mohou být shromažďovány a po dobu 3 měsíců uchovávány údaje o poloze, snímky obrazovky, data o konfiguraci vašeho počítače a data zaznamenaná kamerou počítače.
- Na webu https://my.eset.com je potřeba vytvořit účet, pomocí něhož tato funkce aktivuje sběr dat v případě odcizení počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory.

Důvěrnost údajů

ESET je společnost s celosvětovou působností. Informace, které společnost ESET zpracovává, mohou být přenášeny k přidruženým subjektům nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb, podpora nebo fakturace. Na základě vaší polohy a služeb, které si zvolíte, může být potřeba přenést vaše údaje do země, kde neplatí rozhodnutí Evropské komise o odpovídající ochraně. I v takovém případě každý přenos informací podléhá právním předpisům o ochraně údajů a probíhá pouze v případě potřeby. Bez výjimky musí být stanoveny standardní smluvní doložky, závazná firemní pravidla nebo jiná vhodná ochrana.

Děláme vše pro to, aby nedocházelo k uchovávání dat delší dobu, než je nezbytné k poskytování služeb podle smlouvy EULA. Naše doba uchovávání může trvat déle než platnost vaší licence, a to z toho důvodu, abychom vám poskytli čas pro snadné a pohodlné obnovení. Minimalizované a pseudonymizované statistiky a další data ze služby ESET LiveGrid® mohou být dále zpracovávány pro statistické účely.

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat dozorčí orgány i subjekty údajů. Jako subjekt údajů máte právo podat stížnost u dozorčího orgánu.

Práva subjektu údajů

Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Za podmínek stanovených příslušnými zákony o ochraně údajů máte jako subjekt údajů nárok na následující práva:

- právo požádat společnosti ESET o přístup k vašim osobním údajům,
- právo na opravu vašich osobních údajů, pokud jsou nepřesné (máte také právo na doplnění neúplných osobních údajů),
- právo požadovat vymazání vašich osobních údajů,
- právo požadovat omezení zpracování vašich osobních údajů,
- právo podat námitky proti zpracování,
- právo podat stížnost, stejně tak
- právo na přenositelnost dat.

Věříme, že veškeré informace, které zpracováváme, jsou cenné a nezbytné pro náš legitimní zájem, kterým je poskytování služeb a produktů našim zákazníkům.

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Vedoucí pracovník ochrany osobních údajů
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk