ESET Endpoint Antivirus

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r.o.

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

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

Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována žádným prostředkem, ani distribuována jakýmkoliv způsobem bez předchozího písemného povolení společnosti ESET, spol. s r.o.

ESET, spol. s r.o. si vyhrazuje právo změny programových produktů popsaných v této publikaci bez předchozího upozornění.

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

REV. 2023-03-19

1 ESET Endpoint Antivirus 9 ... 1
1.1 Co je v této verzi nového? ... 2
1.2 Systémové požadavky ... 2
1.2 Podporované jazyky ... 4
1.3 Prevence ... 5
1.4 Nápověda programu ... 6
2 Příručka pro vzdáleně spravované produkty ... 7
2.1 Představení ESET PROTECT ... 8
2.2 Představení ESET PROTECT Cloud ... 9
2.3 Ochrana produktu heslem ... 9
2.4 Co jsou to politiky? ... 10
2.4 Sloučení politik ... 11
2.5 Jak fungují příznaky? ... 11
3 Používání ESET Endpoint Antivirus samostatně ... 12
3.1 Způsoby instalace ... 12
3.1 Instalace včetně ESET AV Remover ... 13
3.1 ESET AV Remover ... 14
3.1 Odinstalace prostřednictvím ESET AV Remover skončila s chybou ... 16
3.1 Instalace (.exe) ... 16
3.1 Změna instalační složky (.exe) ... 18
3.1 Instalace (.msi) ... 18
3.1 Pokročilá instalace (.msi balíček) ... 20
3.1 Minimální instalace ... 21
3.1 Instalace z příkazového řádku ... 22
3.1 Nasazení prostřednictvím GPO nebo SCCM ... 26
3.1 Aktualizace na novou verzi ... 28
3.1 Aktualizace zajišťující bezpečnost a stabilitu ... 29
3.1 Známé problémy při instalaci ... 29
3.1 Neúspěšná aktivace ... 29
3.2 Aktivace produktu ... 30
3.3 Kontrola počítače ... 30
3.4 Začínáme ... 30
3.4 Seznámení s uživatelským prostředím ... 30
3.4 Nastavení aktualizace ... 33
4 Práce s ESET Endpoint Antivirus ... 35
4.1 Počítač ... 37
4.1 Detekční jádro ... 39
4.1 Rozšířená nastavení detekčního jádra ... 43
4.1 Nalezena infiltrace ... 44
4.1 Rezidentní ochrana souborového systému ... 46
4.1 Ověření funkčnosti rezidentní ochrany ... 47
4.1 Kdy měnit nastavení rezidentní ochrany ... 48
4.1 Co dělat, když nefunguje rezidentní ochrana ... 48
4.1 Kontrola počítače ... 48
4.1 Spuštění volitelné kontroly ... 50
4.1 Průběh kontroly ... 52
4.1 Protokol kontroly počítače ... 53
4.1 Detekce škodlivého kódu ... 53
4.1 Kontrola při nečinnosti ... 54
4.1 Profily kontroly ... 54

4.1 Cíle kontroly ... 55
4.1 Rozšířená nastavení kontroly ... 56
4.1 Správa zařízení ... 56
4.1 Editor pravidel ve správě zařízení ... 57
4.1 Detekovaná zařízení ... 58
4.1 Skupiny zařízení ... 58
4.1 Vytvoření nového pravidla ... 59
4.1 Host-based Intrusion Prevention System (HIPS) ... 61
4.1 Interaktivní režim HIPS ... 63
4.1 Detekován potenciální ransomware ... 64
4.1 Správa HIPS pravidel ... 64
4.1 Úprava pravidla HIPS ... 65
4.1 Rozšířená nastavení ... 68
4.1 Ovladače, jejichž načtení je vždy povoleno ... 68
4.1 Prezentační režim ... 68
4.1 Kontrola po startu ... 69
4.1 Automatická kontrola souborů spouštěných při startu počítače ... 69
4.1 Ochrana dokumentů ... 70
4.1 Výjimky ... 70
4.1 Výkonnostní výjimky ... 71
4.1 Přidání a úprava výkonnostních výjimek ... 72
4.1 Formát výjimky podle cesty ... 73
4.1 Detekční výjimky ... 74
4.1 Přidání a úprava detekčních výjimek ... 76
4.1 Průvodce vytvořením detekční výjimky ... 77
4.1 Výjimky (ve verzi 7.1 a starší) ... 78
4.1 Vyloučené procesy ... 78
4.1 Přidání nebo úprava výjimek na procesy ... 79
4.1 HIPS výjimky ... 80
4.1 Parametry skenovacího jádra ThreatSense ... 80
4.1 Úrovně léčení ... 82
4.1 Přípony souborů vyloučených z kontroly ... 83
4.1 Doplňující parametry skenovacího jádra ThreatSense ... 84
4.2 Síť ... 84
4.2 Ochrana proti síťovým útokům ... 85
4.2 Ochrana proti útokům hrubou silou ... 85
4.2 Pravidla ... 86
4.2 Výjimky ... 88
4.2 Rozšířené možnosti filtrování ... 88
4.2 IDS pravidla ... 89
4.2 Zablokovaná podezřelá hrozba ... 91
4.2 Řešení problémů v síťové ochraně ... 91
4.2 Známé sítě ... 92
4.2 Editor známých sítí ... 92
4.2 Autentifikace sítě - konfigurace serveru ... 95
4.2 Seznam dočasně blokovaných IP adres ... 96
4.2 Jak nastavit zóny ... 96
4.2 Zóny firewallu ... 96
4.3 Web a mail ... 97
4.3 Filtrování protokolů ... 98
4.3 Vyloučené aplikace ... 98

4.3 Vyloučené IP adresy ... 99
4.3 SSL/TLS ... 100
4.3 Certifikáty ... 101
4.3 Šifrovaná síťová komunikace ... 102
4.3 Seznam známých certifikátů ... 102
4.3 Seznam SSL/TLS filtrovaných aplikací ... 103
4.3 Ochrana poštovních klientů ... 103
4.3 Poštovní protokoly ... 105
4.3 Značení e-mailů ... 106
4.3 Integrace do poštovních klientů ... 107
4.3 Panel nástrojů v MS Outlook ... 107
4.3 Panel nástrojů v Outlook Express a Windows Mail ... 107
4.3 Potvrzovací dialog ... 108
4.3 Opakovaná kontrola zpráv ... 108
4.3 Ochrana přístupu na web ... 108
4.3 Rozšířená nastavení Ochrany přístupu na web ... 110
4.3 Webové protokoly ... 111
4.3 Správa URL adres ... 111
4.3 Seznam adres ... 112
4.3 Vytvoření nového seznamu ... 113
4.3 Jak přidat masku URL? ... 114
4.3 Anti-Phishingová ochrana ... 115
4.4 Aktualizace programu ... 116
4.4 Nastavení aktualizace ... 120
4.4 Obnovení předchozí verze modulů ... 123
4.4 Aktualizace produktu ... 125
4.4 Možnosti připojení ... 125
4.4 Aktualizační mirror ... 127
4.4 Mirror jako HTTP Server a dostupný prostřednictvím SSL ... 128
4.4 Aktualizace z mirroru ... 129
4.4 Řešení problémů při aktualizaci z mirroru ... 130
4.4 Jak vytvořit aktualizační úlohu ... 131
4.5 Nástroje ... 131
4.5 Protokoly ... 132
4.5 Filtrování protokolů ... 134
4.5 Konfigurace protokolování ... 135
4.5 Audit ... 136
4.5 Plánovač ... 138
4.5 ESET SysInspector ... 140
4.5 Cloudová ochrana ... 141
4.5 Filtr výjimek pro cloudovou ochranu ... 144
4.5 Spuštěné procesy ... 144
4.5 Bezpečnostní přehled ... 145
4.5 ESET SysRescue Live ... 147
4.5 Odeslání vzorku k analýze ... 147
4.5 Podezřelý soubor ... 148
4.5 Podezřelá stránka ... 148
4.5 Falešně detekovaný soubor ... 148
4.5 Falešně detekovaná stránka ... 149
4.5 Ostatní ... 149
4.5 Karanténa ... 149

4.5 Nastavení proxy serveru ... 151
4.5 Časové sloty ... 152
4.5 Aktualizace operačního systému Windows ... 153
4.5 Interval ověření licence ... 154
4.6 Uživatelské rozhraní ... 154
4.6 Prvky uživatelského rozhraní ... 154
4.6 Přístup k nastavení ... 156
4.6 Heslo pro přístup do Rozšířeného nastavení ... 157
4.6 Ikona v oznamovací oblasti ... 158
4.6 Kontextové menu ... 159
4.6 Nápověda a podpora ... 159
4.6 O programu ESET Endpoint Antivirus ... 160
4.6 Odeslat konfiguraci systému ... 161
4.6 Technická podpora ... 161
4.7 Oznámení ... 162
4.7 Stavy aplikace ... 162
4.7 Oznámení na pracovní ploše ... 163
4.7 Dialogové okno – Oznámení na pracovní ploše ... 164
4.7 Přizpůsobení oznámení ... 164
4.7 Interaktivní upozornění ... 164
4.7 Seznam interaktivních upozornění ... 166
4.7 Potvrzovací zprávy ... 167
4.7 Konflikt v rozšířeném nastavení ... 168
4.7 Výměnná média ... 168
4.7 Vyžadován restart ... 169
4.7 Doporučen restart ... 170
4.7 Přeposílání ... 171
4.7 Správa profilů ... 174
4.7 Klávesové zkratky ... 174
4.7 Diagnostika ... 175
4.7 Skener příkazového řádku ... 176
4.7 ESET CMD ... 178
4.7 Detekce stavu nečinnosti ... 181
4.7 Import a export nastavení ... 181
4.7 Obnovit všechna nastavení na standardní ... 182
4.7 Obnovit všechna nastavení v této sekci na standardní ... 182
4.7 Chyba během ukládání nastavení ... 183
4.7 Vzdálené monitorování a správa (RMM) ... 183
4.7 ERMM příkazový řádek ... 184
4.7 Seznam ERMM JSON příkazů ... 185
4.7 get protection-status ... 186
4.7 get application-info ... 186
4.7 get license-info ... 189
4.7 get logs ... 189
4.7 get activation-status ... 190
4.7 get scan-info ... 191
4.7 get configuration ... 192
4.7 get update-status ... 193
4.7 start scan ... 194
4.7 start activation ... 194
4.7 start deactivation ... 195

4.7 start update 196
4.7 set configuration 196
5 Řešení nejčastějších problémů 197
5.1 Nejčastější dotazy týkající se automatické aktualizace produktů 198
5.2 Jak aktualizovat ESET Endpoint Antivirus? 201
5.3 Jak aktivovat ESET Endpoint Antivirus? 201
5.3 Zadání licenčního klíče během aktivace 202
5.3 Přihlášení k ESET Business Account 202
5.3 Jak použít klasické licenční údaje pro aktivaci nové generace produktu ESET? 202
5.4 Jak odstranit vir z počítače? 202
5.5 Jak vytvořit novou úlohu v Plánovači? 203
5.5 Jak naplánovat každý týden kontrolu počítače? 203
5.6 Jak připojit ESET Endpoint Antivirus k ESET PROTECT? 204
5.6 Jak dočasně změnit nastavení vynucené politikou? 204
5.6 Jak aplikovat doporučené politiky pro ESET Endpoint Antivirus? 206
5.7 Jak vytvořit mirror? 208
5.8 Jak přejít na Windows 10 s nainstalovaným ESET Endpoint Antivirus? 208
5.9 Jak aktivovat vzdálené monitorování a správu produktu (RMM)? 209
5.10 Jak zablokovat stahování konkrétních typů souborů? 211
5.11 Jak minimalizovat uživatelské rozhraní ESET Endpoint Antivirus? 212
6 Licenční ujednání s koncovým uživatelem 213
7 Zásady ochrany osobních údajů 220

ESET Endpoint Antivirus 9

ESET Endpoint Antivirus 9 představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ESET LiveGrid® poskytuje rychlou a přesnou ochranu počítače. Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET Endpoint Antivirus 9 je komplexní bezpečnostní řešení, které kombinuje maximální ochranu s minimálním dopadem na operační systém. 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 Antivirus 9 je primárně navržen pro ochranu pracovních stanic v SMB prostředí.

V případě, že budete ESET Endpoint Antivirus používat samostatně, stránky nápovědy jsou pro lepší orientaci logicky uspořádány do jednotlivých kapitol a podkapitol. Naleznete zde informace týkající se stažení, instalace i aktivace produktu.

Pomocí nástroje ESET PROTECT můžete v enterprise prostředí snadno spravovat libovolné množství klientských stanic – aplikovat na ně politiky, sledovat detekce a vzdáleně ESET Endpoint Antivirus 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 Antivirus.
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 Antivirus 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, které mohou obsahovat nevhodný obsah. 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 v této verzi nového?

ESET Endpoint Antivirus 9 si můžete stáhnout a nainstalovat.

Automatické aktualizace

- funkce pro automatickou aktualizaci se stará o to, abyste vždy používali nejnovější verzi produktu
- chytré řešení snižuje údržbu produktu ESET Endpoint Antivirus na minimum
- tato funkce je standardně zapnutá a využívá aktualizaci programových komponent (microPCU)
- neprovádí se přeinstalace produktu, která sebou nese nevýhody v podobě odregistrace ze systému a přenosu konfigurace
- stahuje se menší množství dat (přírůstkové aktualizace)
- přívětivé oznámení pro uživatele jehož zobrazování je možné ve spravovaných sítích potlačit

Dodatky k příslušným licenčním ujednáním s koncovým uživatelem (EULA)

- EULA již není závislá na instalačním procesu a zobrazuje se jako informační prvek v konzoli pro vzdálenou správu nebo uživatelském rozhraní produktu ESET Endpoint Antivirus
- díky tomu jsme zjednodušili proces automatické aktualizace produktu a vylepšili váš uživatelský zážitek, protože již nebude nutné při každé aktualizaci produktu na novou verzi přijímat licenční ujednání s koncovým uživatelem (EULA)

Nativní podpora ARM64

- instalační balíčky verze 9 jsou dostupné pro platformu ARM64

Toto sestavení opravuje řadu chyb a přináší výkonová vylepšení.

Další informace a snímky nových funkcí v produktu ESET Endpoint Antivirus naleznete v Databázi znalostí:

- Co je nového v ESET Endpoint Antivirus 9?

Systémové požadavky

Pro plynulý běh produktu ESET Endpoint Antivirus (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.

Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 s posledními aktualizacemi (alespoň KB4474419 a KB4490628)

> ESET Endpoint Antivirus ve verzi 9.1 je poslední, která má podporu ve Windows 7 a Windows 8.1. Přečtete si článek o používání produktu ESET na zařízeních s Windows 7 and Windows 8.1.

Windows XP a Windows Vista není podporován.

> Vždy se snažte udržovat svůj operační systém aktualizovaný.

> Instalační balíček ESET Endpoint Antivirus vytvořený v ESET PROTECT 8.1 a novější podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 režim 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 1024x768
- 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 Antivirus 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	nn-NO	1044
Polština	pl-PL	1045
Portugalština (Brazílie)	pt-BR	1046
Rumunština	ro-RO	1048
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

Jazyk	Kód jazyka	LCID
Ukrajinština (Ukrajina)	uk-UA	1058
*Vietnamština	vi-VN	1066

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

Pro změnu jazyka této online uživatelské příručky použijte menu pro výběr jazyka (v pravém horním rohu).

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 infiltrací většinou neberou ohled na potřeby uživatelů. 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. To znamená, že při každém přístupu k souboru, dojde 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 nápovědě k ESET Endpoint Antivirus. Věříme, že informace obsažené v této nápovědě vás seznámí s produktem a pomohou vám zabezpečit počítač.

Jak začít

Před zahájením používání ESET Endpoint Antivirus nezapomeňte na to, že produkt můžete připojit do ESET PROTECT nebo jej používat samostatně. 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 Antivirus si můžete přečíst zde. Připravili jsme také průvodce, který vám pomůže se základním nastavením ESET Endpoint Antivirus.

Jak používat nápovědu programu ESET Endpoint Antivirus

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 Antivirus. 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 Antivirus 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 Antivirus můžete vzdáleně spravovat prostřednictvím ESET PROTECT nebo ESET Cloud Administrator.

- Představení ESET PROTECT
- Představení ESET PROTECT Cloud

Nástroje třetích stran pro vzdálenou správu

- Vzdálené monitorování a správa (RMM)

Best practices

- Připojte všechny stanice s nainstalovaným ESET Endpoint Antivirus 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 Antivirus uživateli

Jak na to

- Jak dočasně změnit nastavení vynucené politikou?
- Jak nasadit ESET Endpoint Antivirus 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 instalovat bezpečnostní řešení ESET na zařízení, spravovat jejich konfiguraci a rychle reagovat na nové problémy a detekce v síti. Seznamte se s ESET PROTECT architekturou a jednotlivými prvky infrastruktury, podporovanými Desktop Provisioning prostředími a následně přejděte do kapitoly Začínáme s ESET PROTECT Web Console.

ESET PROTECT se skládá z následujících komponent:

- ESET PROTECT Server – můžete jej nainstalovat na Windows, Linux nebo do virtuální prostředí nasadit jako virtuální appliance. Výkonná část, která zajišťuje komunikaci mezi klientskými stanicemi (agenty) a uchovává data v databázi.
- ESET PROTECT 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. 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 Management Serverem. ESET PROTECT Agenta musíte nainstalovat na každé zařízení, které chcete vzdáleně spravovat prostřednictvím ESET PROTECT Web Console. Agenta je třeba nainstalovat na každé klientské zařízení pro navázání komunikace mezi ním a ESET PROTECT Serverem. Díky agentovi jste schopni ze stanici získat mnohem větší množství dat, a protože si agent pamatuje veškeré politiky, odpovídající nastavení aplikuje v případě detekce okamžitě bez nutnosti přímé viditelnosti ESET ManagementESET_PROTECT Serveru. 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. Agenta také můžete na stanice instalovat ručně.
- Rogue Detection Sensor – ESET Rogue Detection Sensor (RD Sensor) je nástroj, který vyhledává zařízení v síti a představuje pohodlný způsob pro přidání nových počítačů do ESET PROTECT bez nutnosti jejich ručního zadávání. Představuje pohodlný způsob pro přidání nových počítačů do konzole bez nutnosti jejich ručního zadávání. RD Sensor si pamatuje počítače, které již objevil, a neodesílá duplicitní informace.
- Apache HTTP Proxy – 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, která zajišťuje komunikaci mezi ESET PROTECT a mobilními zařízení s OS Android (a aplikací ESET Endpoint Security pro Android) případně operačním systémem iOS.
- ESET PROTECT Virtuální appliance – připravený virtuální stroj založený na operačním systému CentOS 7 s ESET PROTECT (ESET PROTECT) určený pro provoz ve virtuálním prostředí.
- ESET PROTECT Virtual Agent Host – komponenta ESET PROTECT, která virtualizuje agenty chráněných virtuálních strojů ve VMware prostředí prostřednictvím produktu ESET Virtualization Security. 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 sítě bez přístupu k internetu. Prostřednictvím tohoto nástroje vytvoříte lokální kopii aktualizačních serverů i online repozitáře s instalačními balíčky.
- 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.

- ESET Business Account (ESET Business Account) – nový licenční portál, prostřednictvím kterého můžete spravovat všechny své licence. Pro více informací o aktivaci bezpečnostních produktů přejděte do kapitoly ESET Business Account v této příručce, případně se podívejte do uživatelské příručky k samotnému portálu ESET Business Account. Pokud máte k dispozici pouze uživatelské jméno a heslo, na tomto portále si je můžete převést na licenční klíč.
- ESET Inspect – je komplexní EDR (Endpoint Detection and Response) 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.

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.

Pro více informací se podívejte do online uživatelské příručky k 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.

- Pro více informací přejděte do online uživatelské příručky k ESET PROTECT Cloud.

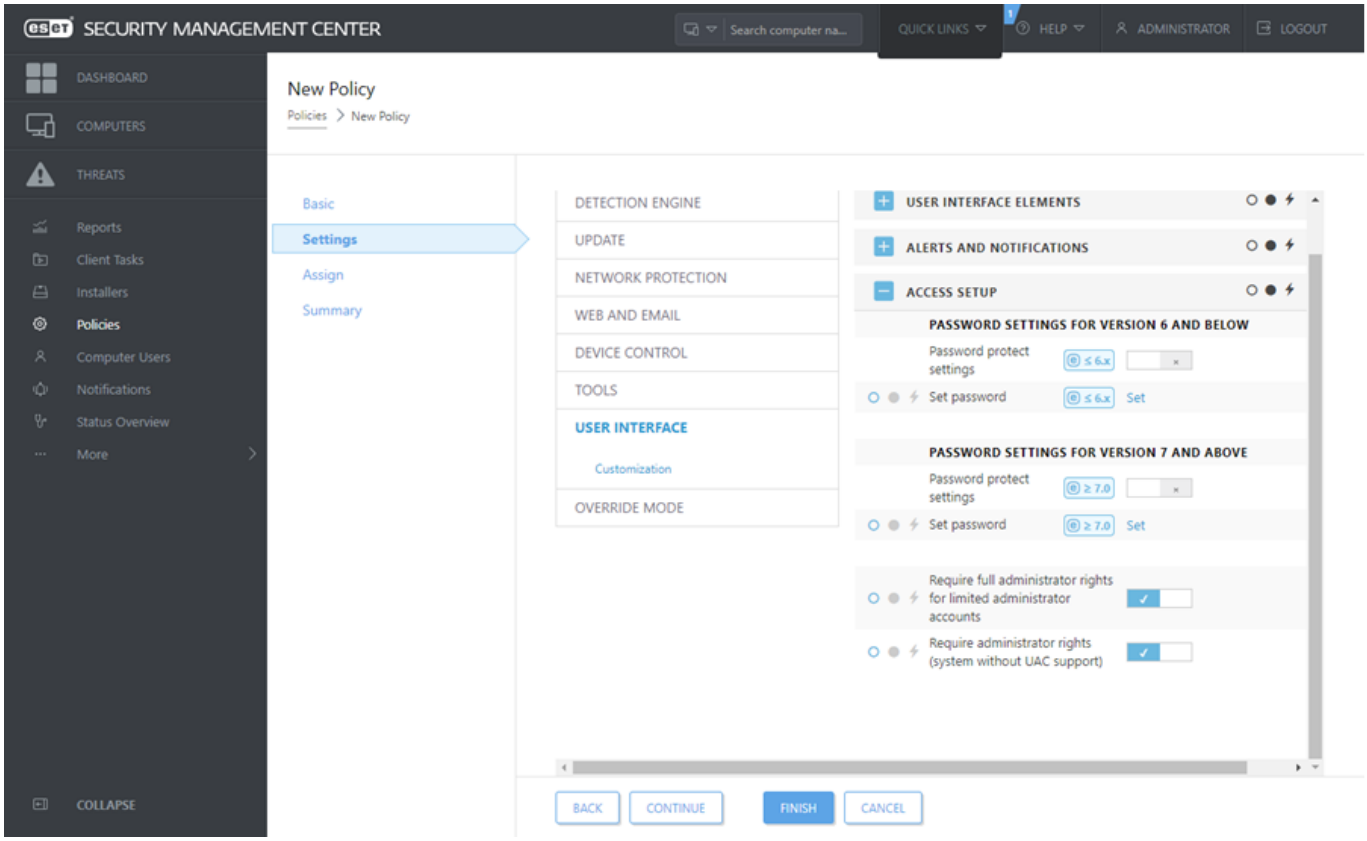
Ochrana produktu heslem

Pro zajištění maximálního zabezpečení systému je nutné zajistit správnou konfiguraci ESET Endpoint Antivirus. 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 Antivirus. 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 používané verzi produktu ESET Endpoint Antivirus aktivujte odpovídající přepínač u možnosti **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 dialogovém okně 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 Antivirus 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 Antivirus 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**.

Používání ESET Endpoint Antivirus samostatně

Tato část příručky stejně jako Práce s ESET Endpoint Antivirus je určena uživatelům, kteří ESET Endpoint Antivirus používají bez napojení do ESET PROTECT nebo ESET PROTECT Cloud. Přístup k jednotlivým funkcím a součástem produktu ESET Endpoint Antivirus závisí na oprávnění uživatele v operačním systému.

Způsoby instalace

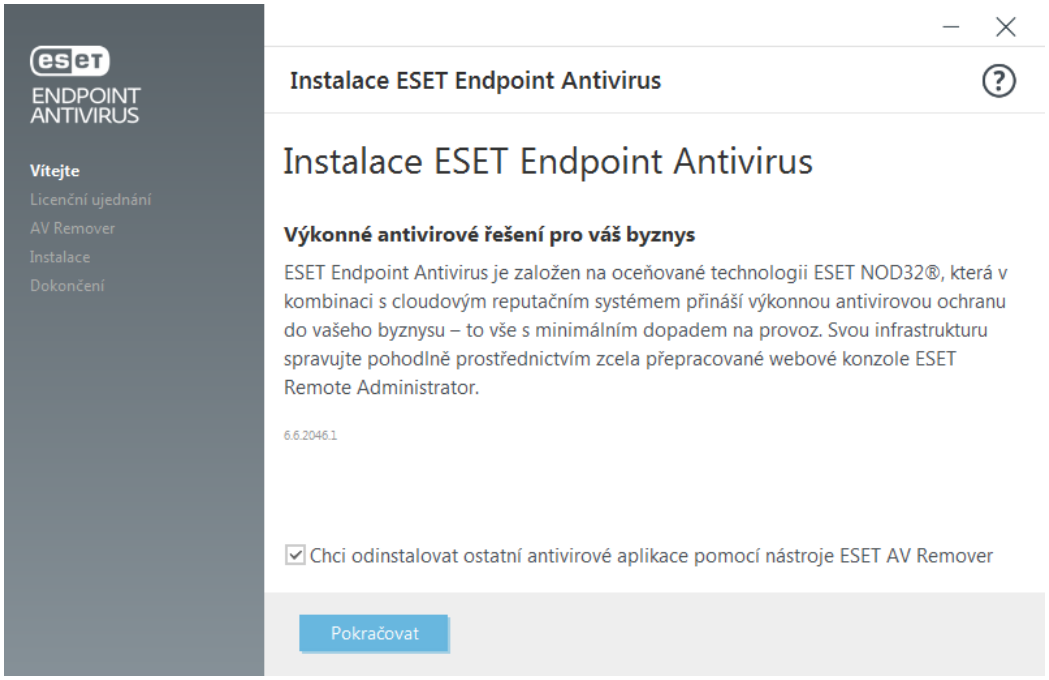
ESET Endpoint Antivirus ve verzi 9 můžete na stanici nasadit mnoha způsoby, bez ohledu na to, zda ji spravujete vzdáleně prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud.

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 64-bit Stáhnout 32-bit
.exe balíček	Instalace bez spuštění ESET AV Remover.	N/A
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 64-bit Stáhnout 32-bit
Instalace z příkazového řádku	ESET Endpoint Antivirus 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 Antivirus 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 Antivirus.	N/A

ESET Endpoint Antivirus je dostupný ve více než 30 jazycích.

Instalace včetně ESET AV Remover

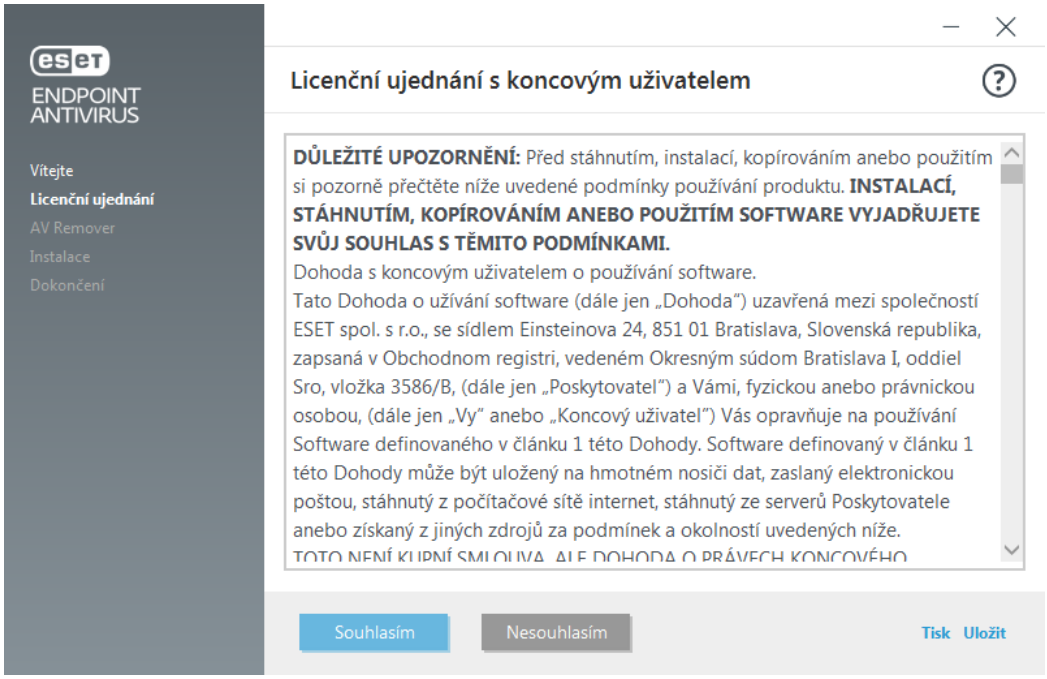
Je důležité, abyste před instalací produktu ESET odinstalovali jiné bezpečnostní aplikace, jejichž součástí jsou prvky rezidentní ochrany (například antivirové a antispywarové programy, firewall). Současné používání několika takových aplikací může vést k vážným konfliktům. Po spuštění instalace vyberte 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 Antivirus bez nástroje ESET AV Remover.



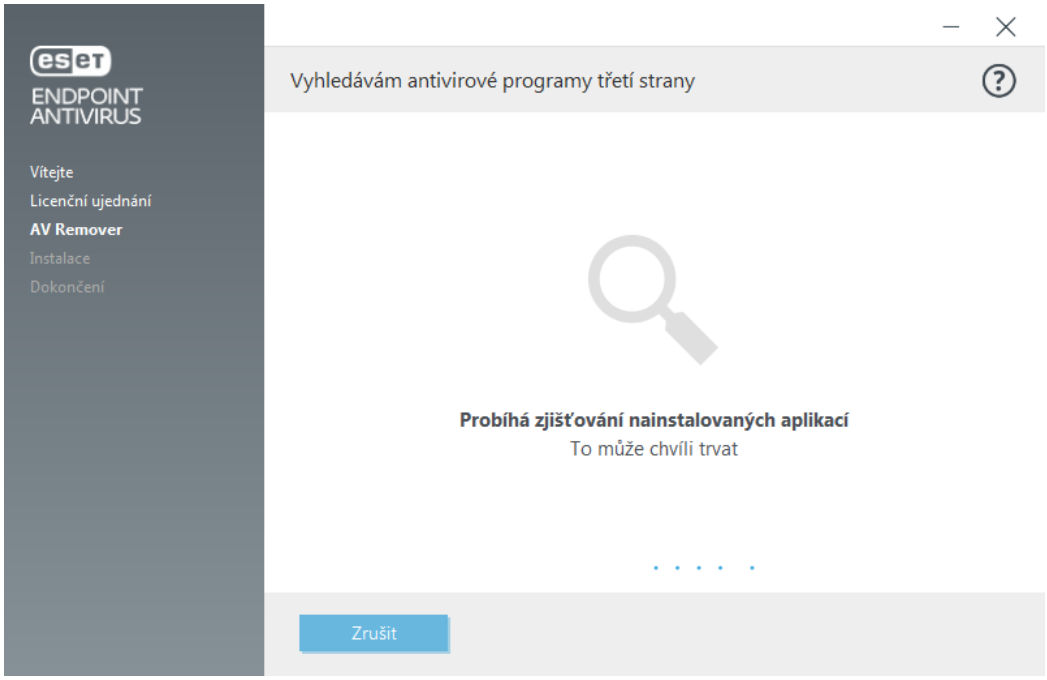
ESET AV Remover

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:

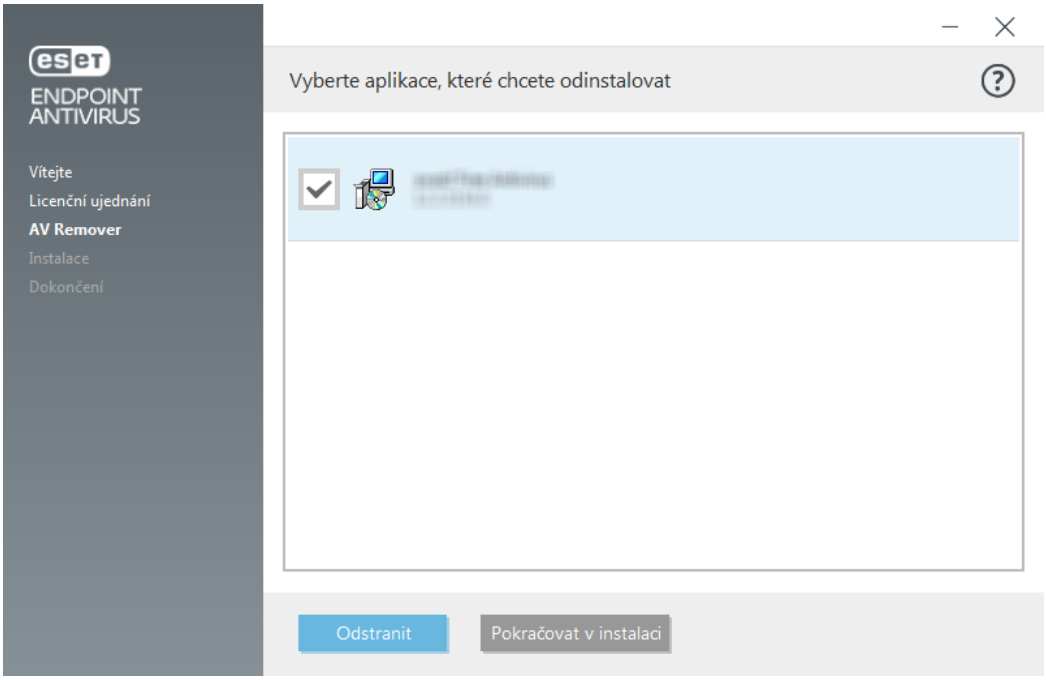
1. Seznam aplikací, které ESET AV Remover podporuje, naleznete v ESET Databázi znalostí.
2. Po kliknutí na tlačítko **Přijmout** nástroj ESET AV Remover prohledá váš počítač. Pokud kliknete na **Nesouhlasím**, bude pokračovat instalace ESET Endpoint Antivirus bez odebrání již existujících produktů v systému.



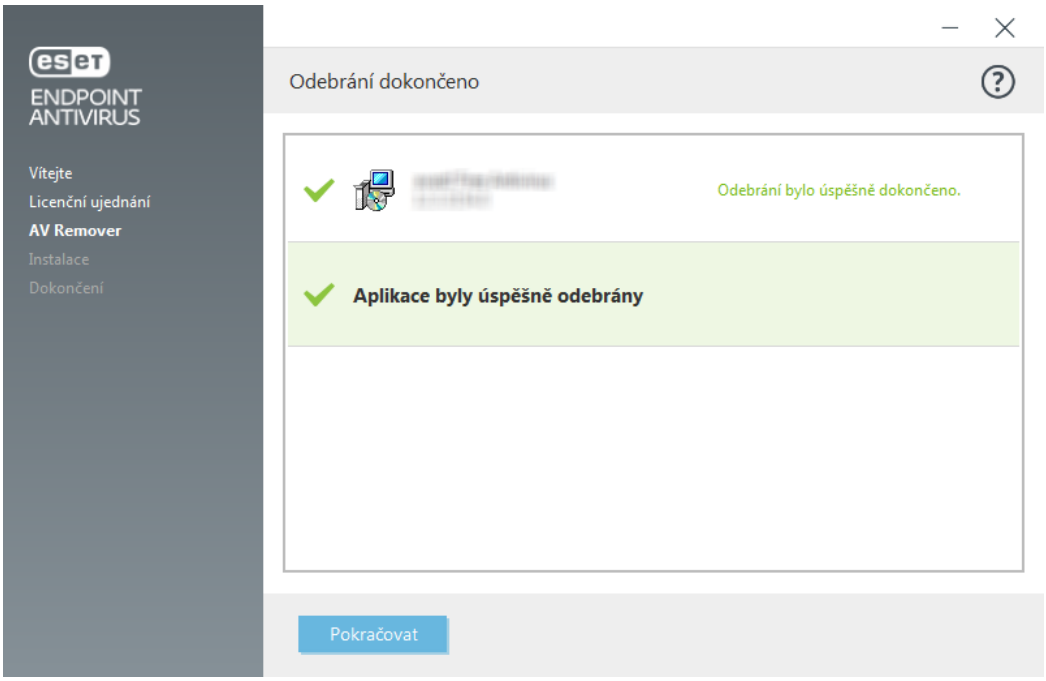
2. ESET AV Remover se pokusí ve vašem systému najít jiná antivirová řešení.



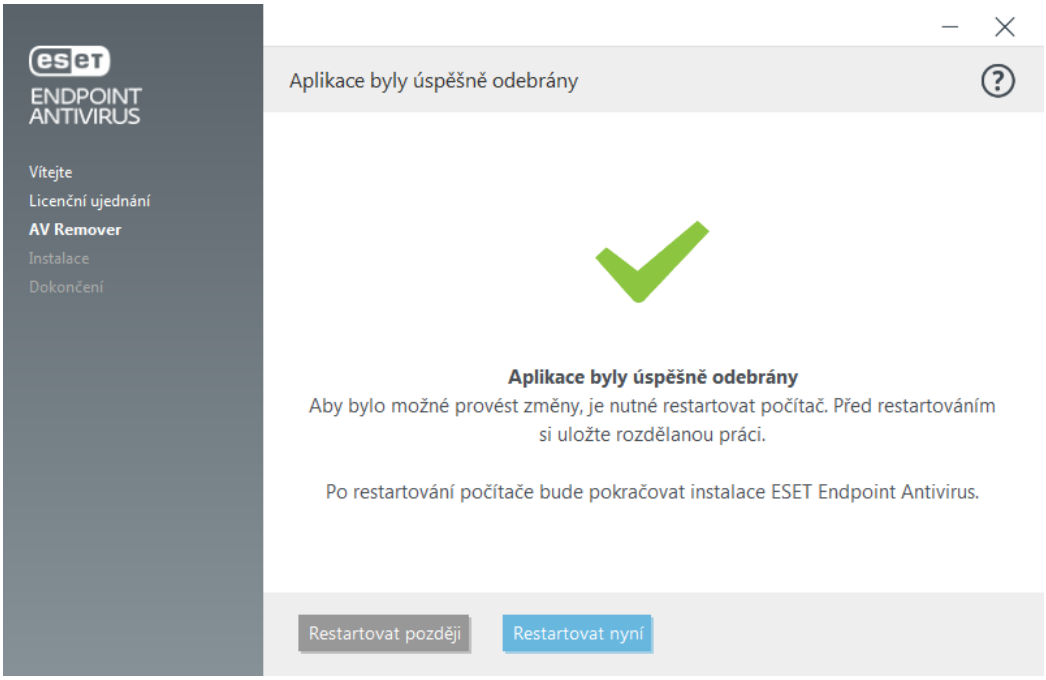
2. Vyberte aplikace, které chcete odebrat ze systému a klikněte na tlačítko **Odebrat**. Tato akce může chvíli trvat.



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



6. Pro dokončení změn v systému restartujte počítač a poté pokračujte instalací ESET Endpoint Antivirus. 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.

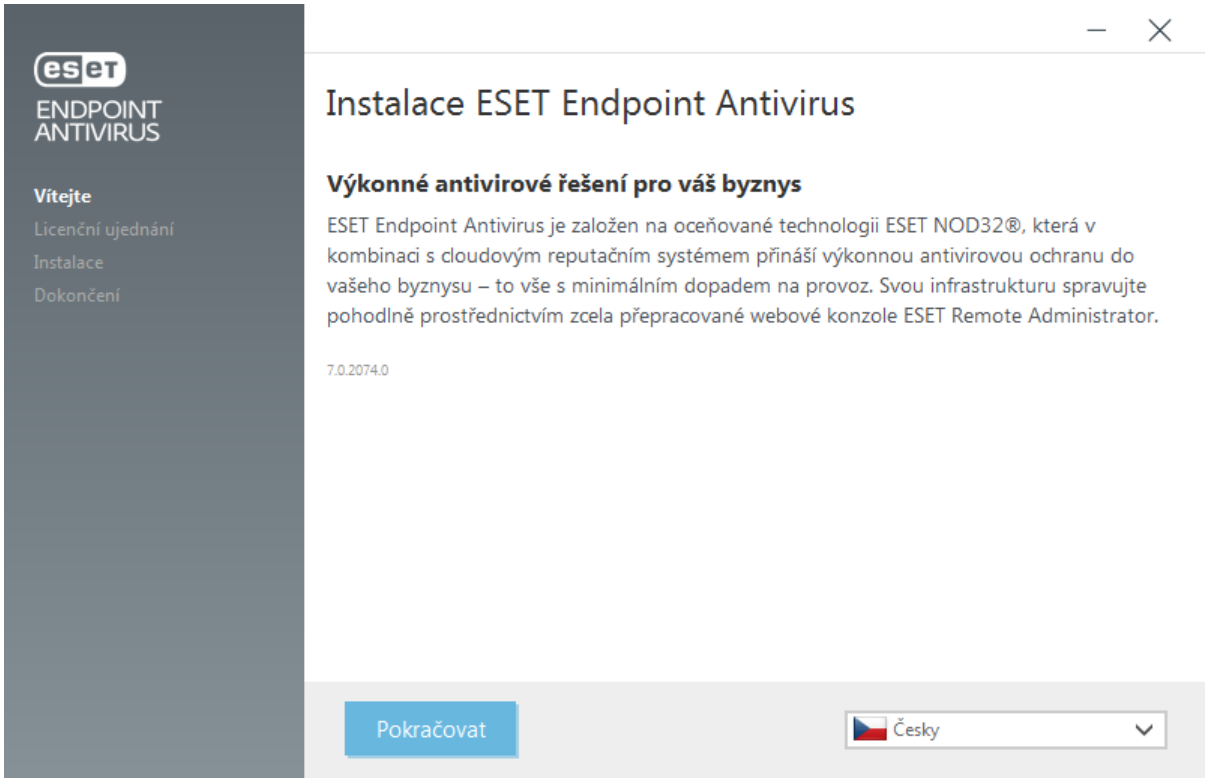
Při neúspěšné odinstalaci jiného bezpečnostního produktu mohly v systému zůstat jeho zbytky. Proto budete vyzváni k **restartování počítače a provedení nové kontroly** na přítomnost těchto pozůstatků. Proto budete vyzváni k restartování počítače a provedení nové kontroly na přítomnost těchto pozůstatků.

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.

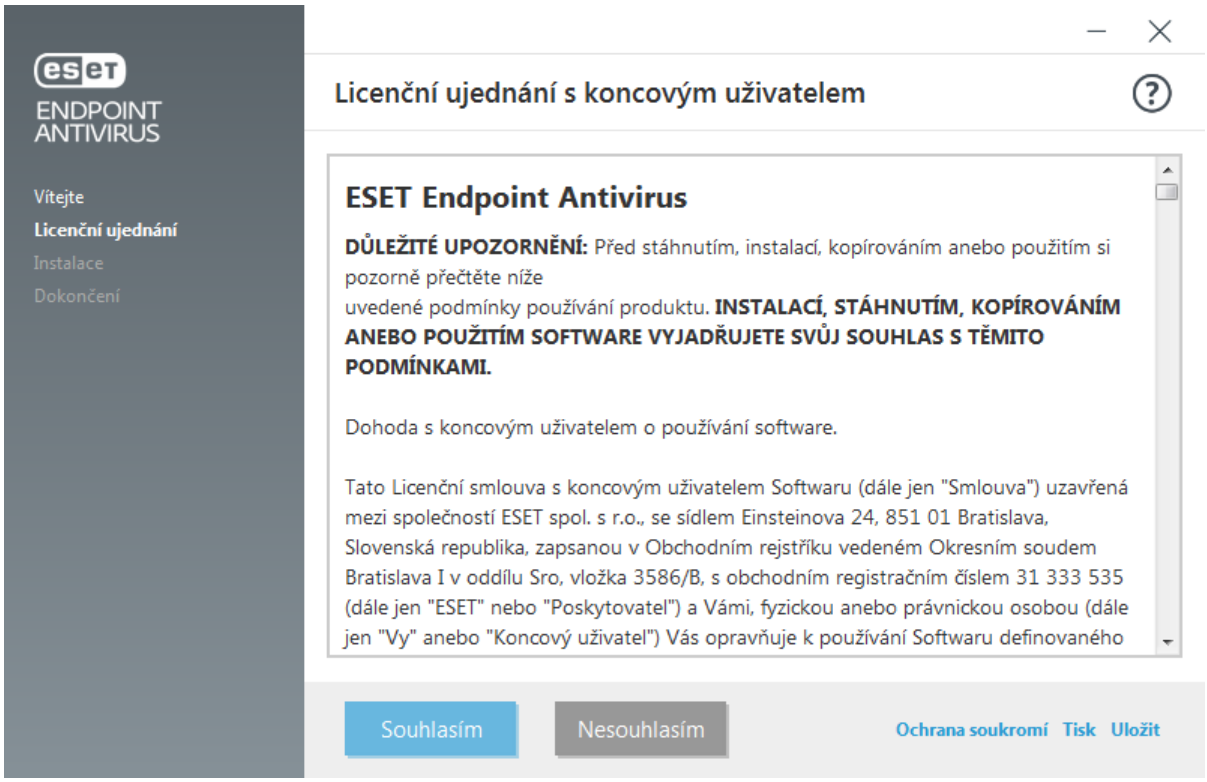
Instalace (.exe)

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. Přečtěte si licenční ujednání s koncovým uživatelem. Pokud chcete zapnout detekci potenciálně nechtěných aplikací a zapojit se do systému zpětné vazby ESET LiveGrid®, klikněte na tlačítko **Přijmout vše a pokračovat**. 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. Kliknutím na tlačítko **Pokračovat** potvrdíte váš souhlas s Licenční ujednáním s koncovým uživatelem. Pokud chcete ESET Endpoint Antivirus nainstalovat do jiné než výchozí složky, klikněte na **Změnit instalační složkuPRODUCTNAME**.



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

Změna instalační složky (.exe)

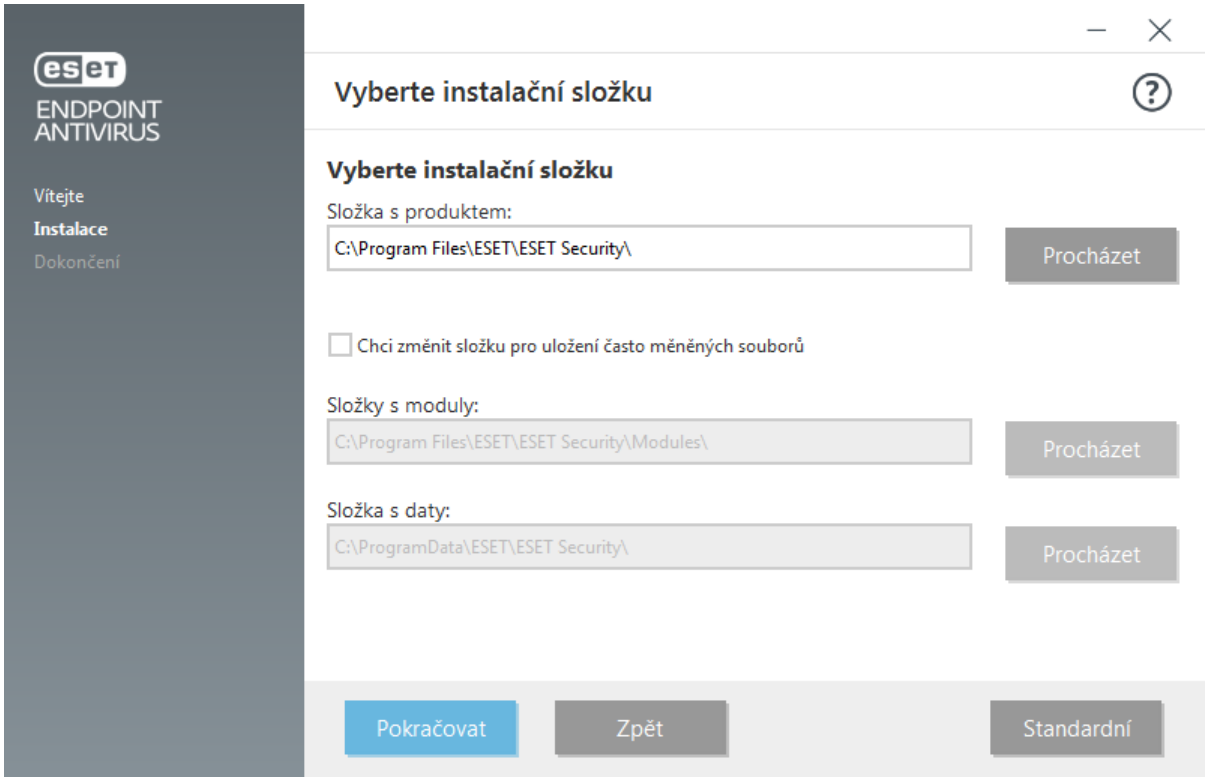
Po nastavení detekce potenciálně nechtěných aplikacích kliknutím na tlačítko **Změnit instalační složku** můžete vybrat složku, do které se má ESET Endpoint Antivirus nainstalovat. Standardně se program instalujte do následující složky:

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)

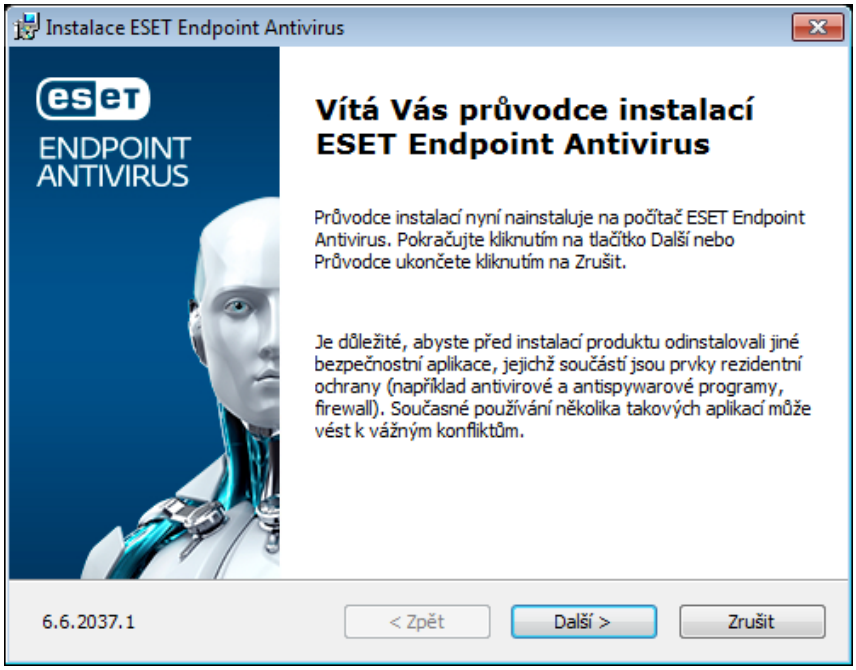
Po spuštění .msi instalačního balíčku se zobrazí průvodce, který vás provede celým procesem instalace.

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.

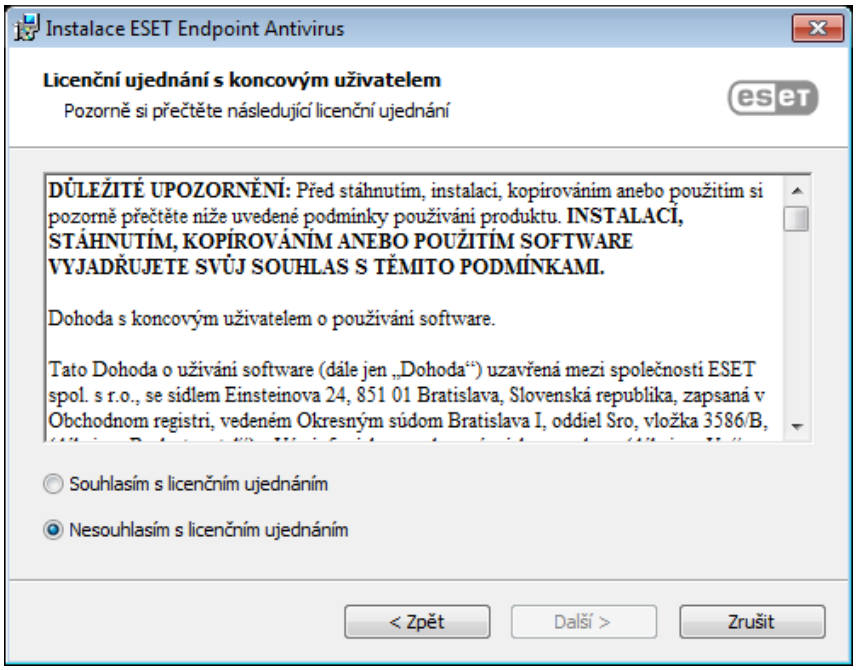
Ujistěte se, zda nemáte nainstalován další antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě. Proto doporučujeme odinstalovat všechny ostatní antivirové programy. V databázi znalostí naleznete nástroje pro odinstalaci nejrozšířenějších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

Instalační balíček ESET Endpoint Antivirus vytvořený v ESET PROTECT 8.1 a novější podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 režim více relací.

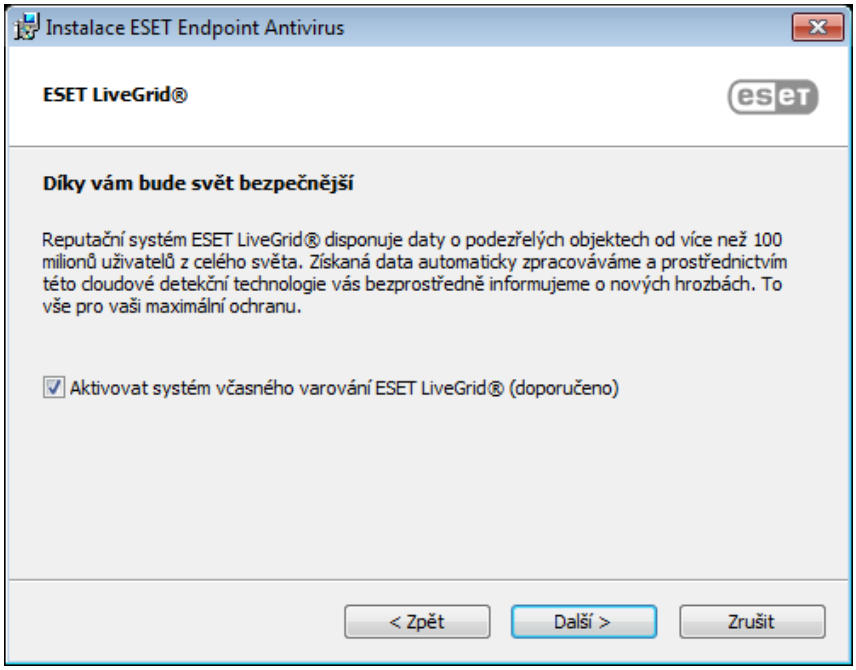
1. Vyberte si požadovaný jazyk a klikněte na tlačítko **Další**.



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 pokračovat Pokročilou instalací (.msi balíčku), klikněte na tlačítko **Pokročilé nastavení**.



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

Pokročilá instalace (.msi balíček)

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

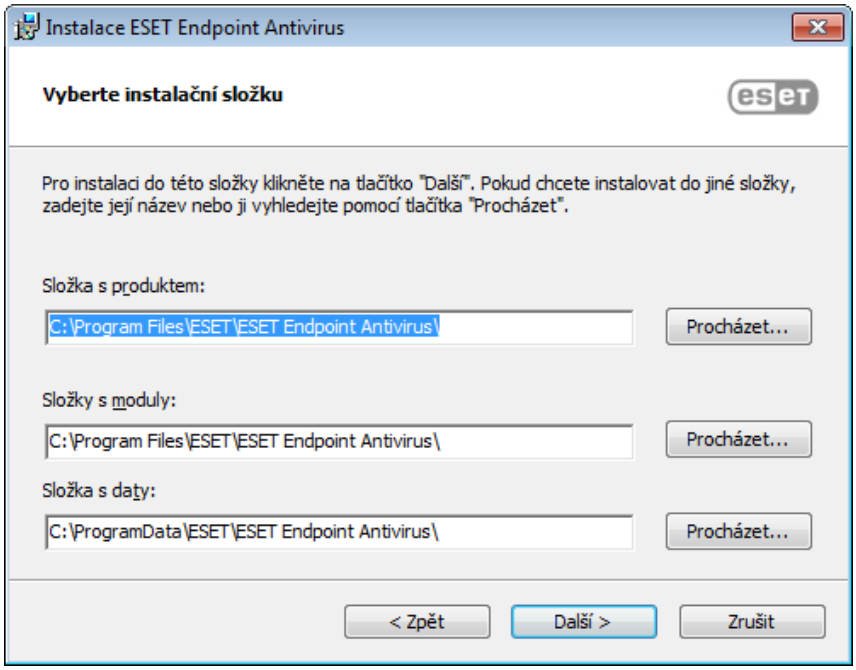
5. Po nastavení detekce potenciálně nechtěných aplikacích kliknutím na tlačítko **Pokročilé nastavení** zpřístupníte pokročilý režim instalace. V dalším kroku můžete změnit složku, do které se má ESET Endpoint Antivirusnainstalovat. Standardně se program instalujte do následující složky:

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).



7. Kliknutím na tlačítko **Instalovat** zahájíte instalaci produktu.

Minimální instalace

Za účelem snížení množství přenášených dat souvisejících s instalačním balíčkem produktu ESET Endpoint Antivirus 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 podpory technologie Anti-Stealth
- Modul Direct Cloud komunikace
- Modul jazykové lokalizace
- Modul konfigurace
- Modul podpory kryptografického protokolu

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**.

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

V případě, že dojde k selhání inicializačního procesu a nejste schopni stáhnout zbývající moduly, použije úplný MSI instalační balíček.

Instalace z příkazového řádku

ESET Endpoint Antivirus 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 Antivirus:

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
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	`Antispam`	`EmailClientProtection`	Volitelná
Web a mail / Filtrování obsahu webu	`WebControl`	`WebAndEmail`	Volitelná

Popis	Název komponenty	Nadřazená komponenta	Přítomnost
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
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*)

Vlastnost LiveGrid®

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

Funkce	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Reputační systém ESET LiveGrid®	Zapnuto	Zapnuto

Funkce	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
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 Antivirus (definovat je nutné oba parametry)

Vlastnost	Hodnota
`PRODUCT_LANG=`	LCID desítkové číslo (Locale ID). Například 1029 pro češtinu, viz seznam jazykových kódů.
`PRODUCT_LANG_CODE=`	LCID řetězec (Language Culture Name) uvedený malými písmeny. Například cs-cz pro češtinu, viz seznam jazykových kódů.

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 Antivirus automaticky nakonfigurovat po dokončení instalace, použijte v instalačním příkazu základní konfigurační parametry.
Instalace ESET Endpoint Antivirus 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 Antivirus 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 Antivirus 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 Antivirus. 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 Antivirus.

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 Antivirus přímo. Nicméně nejedná se o doporučený způsob, protože nemáte k dispozici přehled o stavu produktu a nemůžete na něj prostřednictvím politik vynutit požadované nastavení.

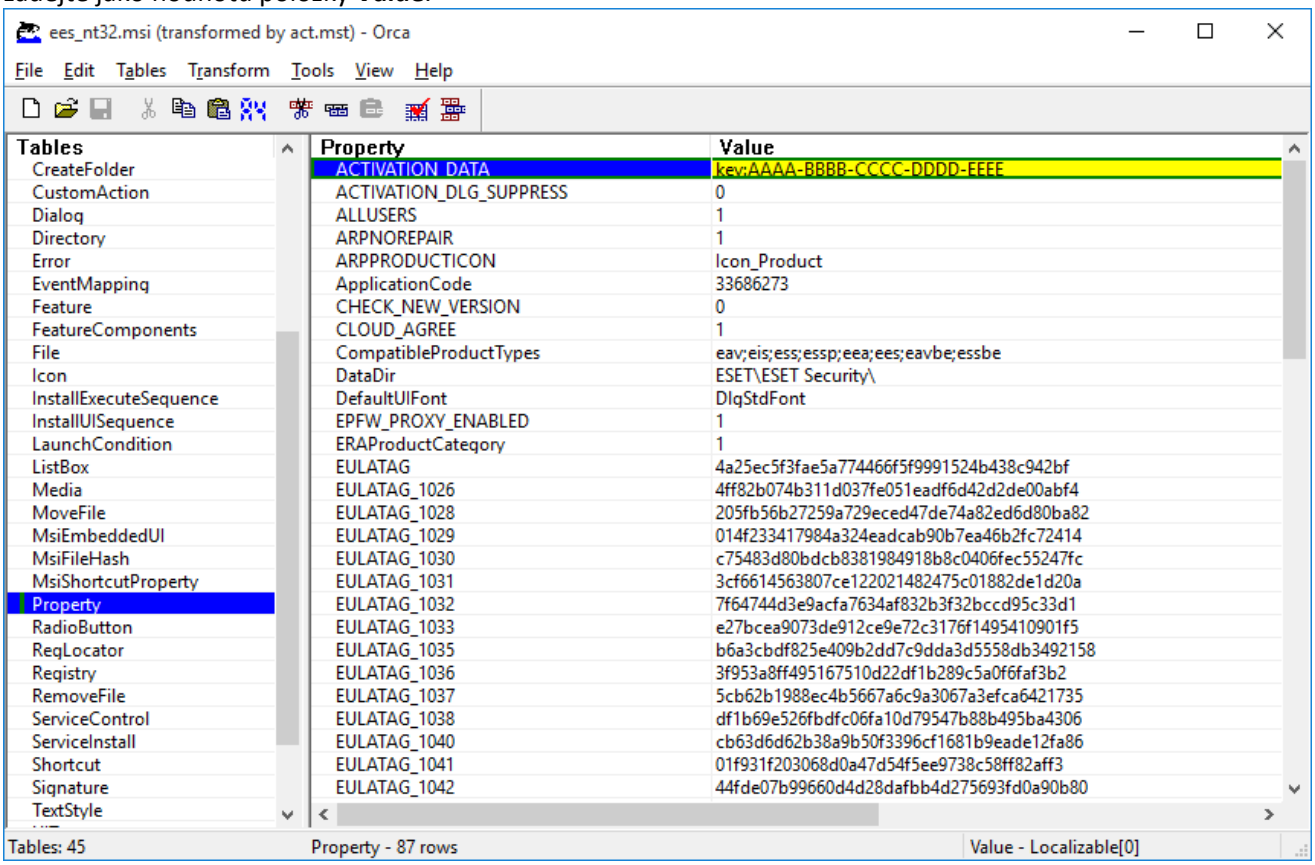
Po dokončení instalace není produkt ESET Endpoint Antivirus standardně aktivován a funkční.

Možnost 1 (Instalace aplikace)

1. Stáhněte si .msi instalační balíček produktu ESET Endpoint Antivirus.
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 Antivirus 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 Antivirus.
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 Antivirus 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 Antivirus 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 Antivirus 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. Automaticky prostřednictvím ESET PROTECT nebo ESET PROTECT Cloud. ESET Endpoint Antivirus ve verzi 9 není možné spravovat prostřednictvím ESET Remote Administrator.
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 **Rozšířeném nastavení** (F5) v sekci **Aktualizace** > **Obecné** > **Aktualizace produktu** aktivní možnost **Automatické 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.

Pro více informací si přečtěte níže uvedené kapitoly z uživatelských příruček:

- 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

Neinstalujte verzi 9.x přes 4.x. Podobně, pokud máte starší/nefunkční ESET Endpoint Antivirus ve verzi 5.x nebo 6.x.

Pokud jste se rozhodli pro ruční aktualizaci:

1. Ověřte, zda máte podporovaný operační systém (Windows Vista a Windows XP již tato verze produktu nepodporuje).

2. Stáhněte si a nainstalujte nejnovější verzi přes stávající.

Pokud chcete minimalizovat riziko selhání procesu aktualizace na poslední verzi 9.x, provádějte aktualizaci z níže uvedených verzí ESET Endpoint Antivirus:
• 5.0.2272.x
• 6.5.2132.x
• 7.3.2044.x
V ostatních případech nejprve stávající verzi produktu ESET Endpoint Antivirus odinstalujte. Pro více informací týkající se aktualizace přejděte do Databáze znalostí.

Aktualizace zajišťující bezpečnost a stabilitu

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

Známé problémy při instalaci

Pokud se při instalaci produkt ESET vyskytne problém, zkuste řešení najít v Databázi znalostí.

Neúspěšná aktivace

V případě, že se produkt ESET Endpoint Antivirus nepodařilo úspěšně aktivovat, níže uvádíme nejčastější příčiny:

- Licenční klíč je již používán.
- Neplatný licenční klíč. Chyba aktivačního formuláře.
- Chybějící nebo špatně zadané doplňující informace k aktivačnímu klíči.
- Komunikace s aktivační databází se nezdařila. Prosím, zkuste to za 15 minut.
- Žádné nebo blokované spojení s ESET aktivačními servery.

Ujistěte se, že jste správně zadali Licenční klíč nebo použili platný Offline soubor, a zkuste to 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

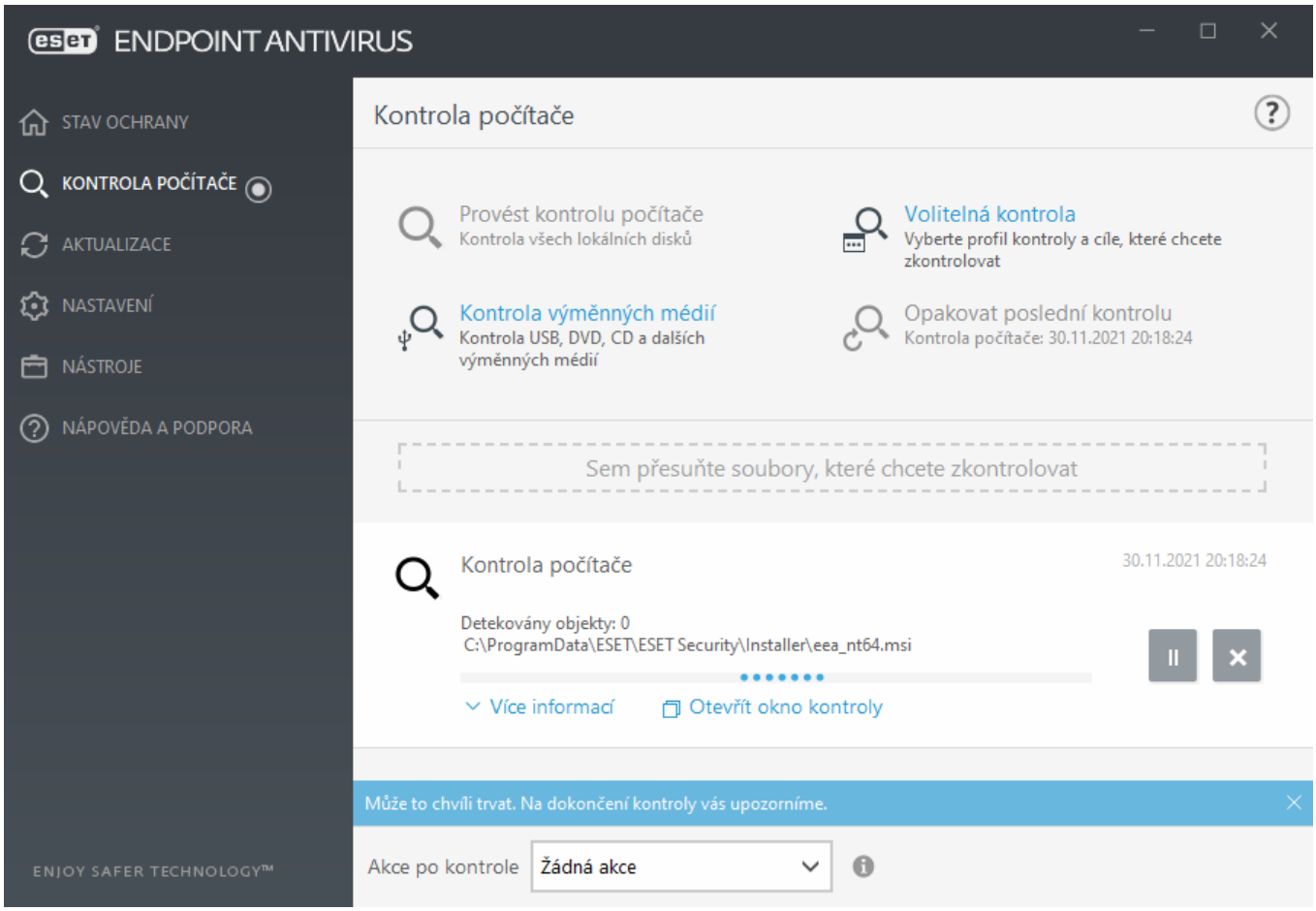
Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu.

Vyberte jednu z dostupných metod pro aktivaci ESET Endpoint Antivirus. Více informací naleznete v kapitole Jak aktivovat ESET Endpoint Antivirus?

Kontrola počítače

Doporučujeme pravidelně provádět kontrolu počítače, případně si naplánovat pravidelnou kontrolu. Pro spuštění kontroly přejděte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Provést kontrolu počítače**. Více informací naleznete v kapitole Kontrola počítače.



Začínáme

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

Seznámení s uživatelským prostředím

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

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

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

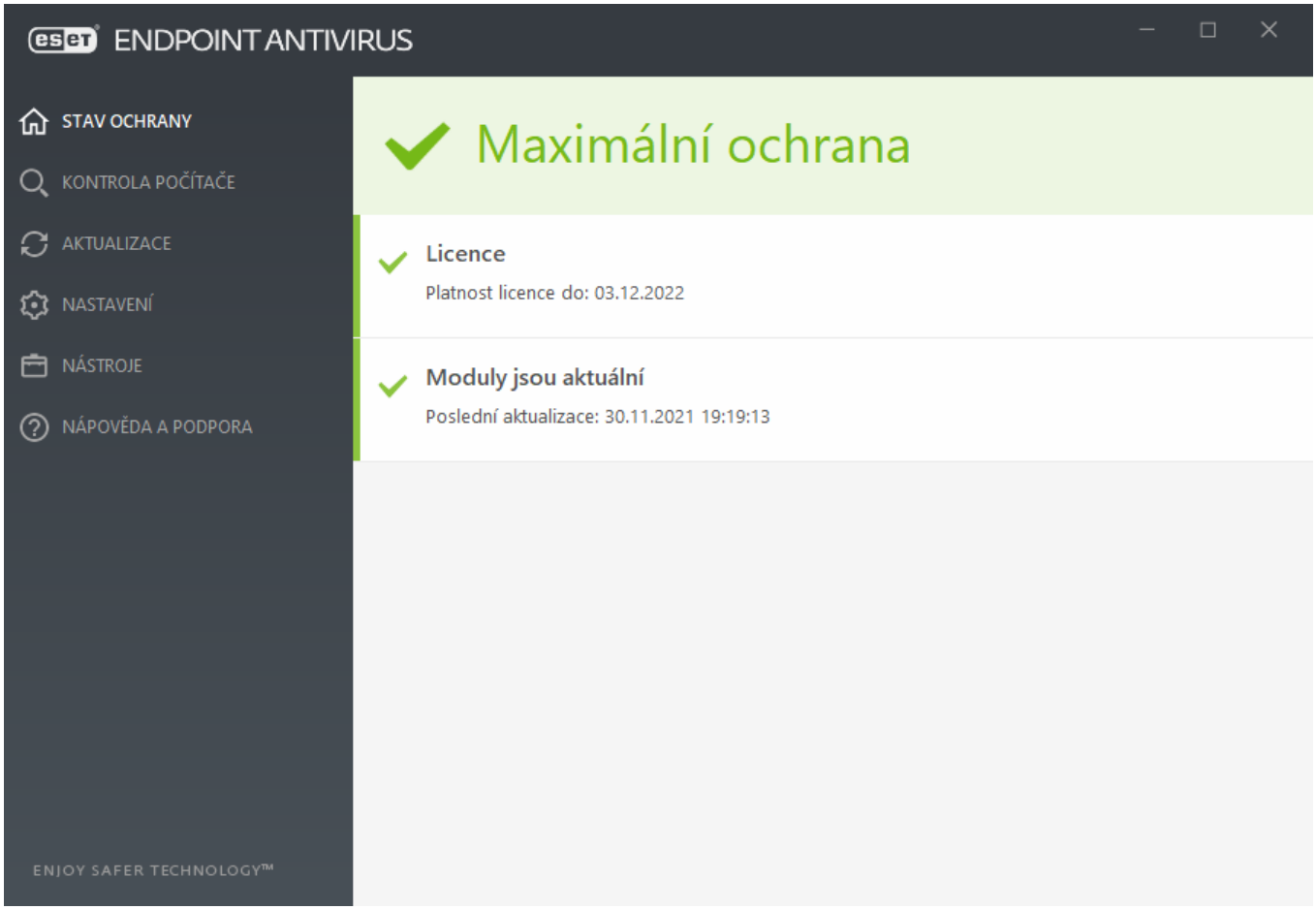
Kontrola počítače – v této části můžete spustit kontrolu svého počítače, definovat parametry vlastní kontroly, stejně tak provést kontrolu výměnných médií. Také můžete zopakovat naposledy provedenou kontrolu.

Aktualizace – zobrazuje informace o aktualizaci detekčního jádra a dalších programových modulů, a nabízí možnost pro ruční kontrolu dostupnosti aktualizací.

Nastavení – obsahuje možnosti nastavení ochrany pro Počítač. a Web a mail.

Nástroje – zajišťuje přístup k protokolům, statistikám ochrany, sledování aktivity, spuštěným procesům, plánovači, karanténě, nástroji ESET SysInspector a ESET SysRescue pro vytvoření záchranného CD. Dále zde naleznete možnost pro odeslání vzorku k analýze do virových laboratoří společnosti ESET.

Nápověda a podpora – poskytuje přístup k nápovědě, ESET Databázi znalostí a webové stránce společnosti ESET. Dále zde můžete přímo vytvořit dotaz na technickou podporu, v dolní části okna naleznete diagnostické nástroje a informace o aktivaci produktu.

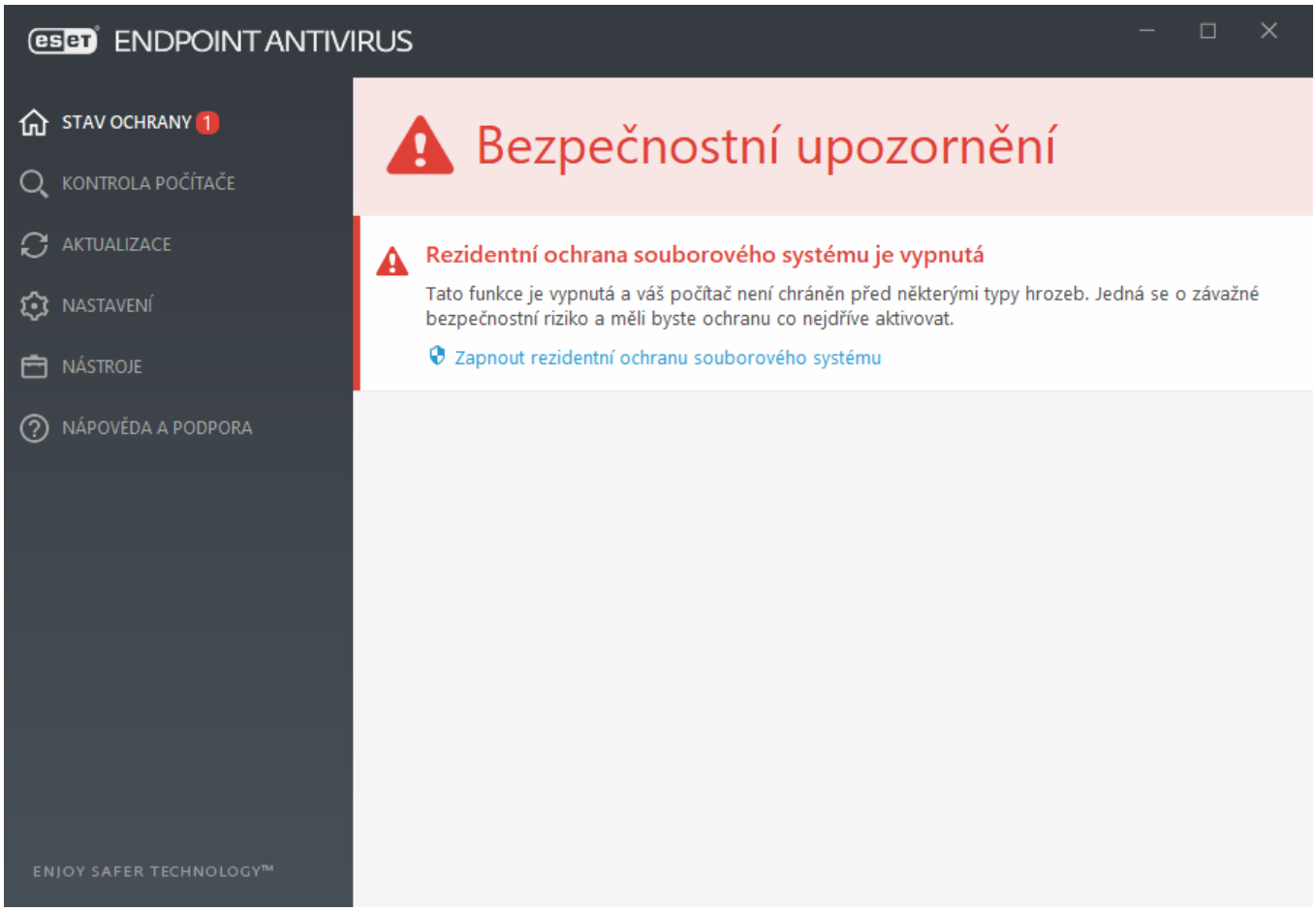


Na záložce **Stav ochrany** jsou zobrazeny informace o bezpečnosti a úrovni ochrany počítače. Zelená ikona a informace **Maximální ochrana** znamená, že je zajištěna maximální úroveň ochrany.

V tomto okně dále naleznete odkazy na často používané funkce ESET Endpoint Antivirus a informace o poslední aktualizaci virové databáze.

Co dělat, pokud systém 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 Antivirus nebude funkční.
- **Anti-Phishingová ochrana není funkční** – tato funkce vyžaduje další součásti programu, které neběží.
- **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 **Platnost licence vypršela** – ikona 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 poukazuje na stav, kdy je HIPS vypnutý v rozšířeném nastavení produktu. Váš počítač není chráněn proti některým hrozbám a ochranu byste měli co nejdříve aktivovat kliknutím na možnost **Zapnout HIPS**.

- **ESET LiveGrid® je vypnutý** – v rozšířeném nastavení aktivujte kontrolu souborů vůči cloudovému reputačnímu systému.
- **Není naplánována pravidelná aktualizace** – ESET Endpoint Antivirus nebude automaticky kontrolovat dostupnost aktualizací.
- **Technologie Anti-Stealth je vypnutá** – pro její aktivování klikněte na **Zapnout Anti-Stealth**.
- **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** – v tomto případě ikona ochrany změní barvu na žlutou a zobrazí vysvětlení. Poté, co licence vyprší, se program přestane aktualizovat a ikona ochrany změní barvu na červenou.
- **Antispamová ochrana je dočasně vypnutá** – pro vyřešení klikněte na možnost **Zapnout antispamovou ochranu**.
- **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 Antivirus přejděte do kapitoly Stavy aplikace.

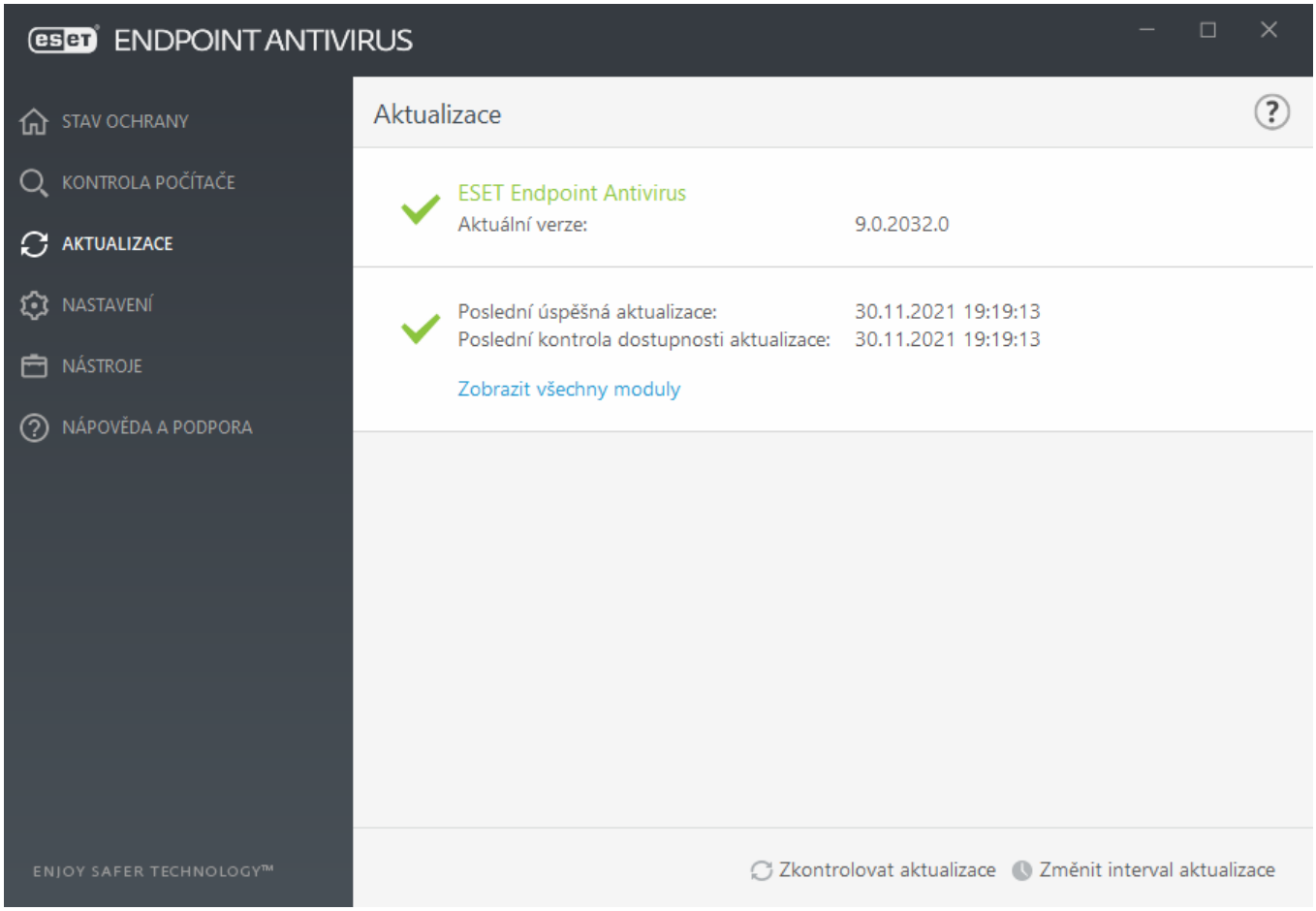
Pokud uvedený návrh na řešení problému nezabral, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zobrazte nápovědu nebo přejděte do ESET Databáze znalostí. Pokud i přesto budete potřebovat pomoc, můžete odeslat dotaz na technickou podporu. Specialisté technické podpory ESET vám odpoví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

Nastavení aktualizace

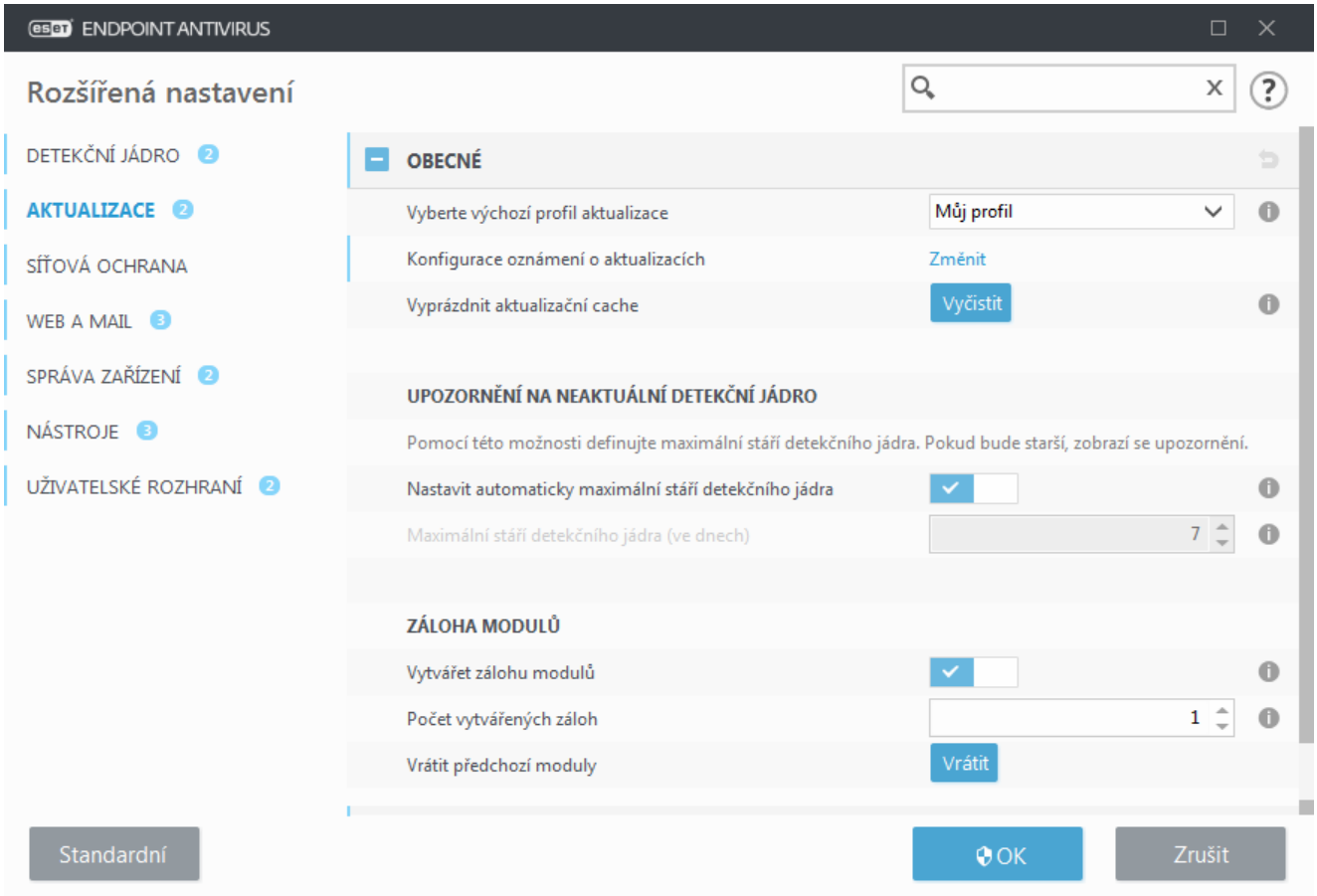
Aktualizace detekčních a programových modulů je důležitá pro zajištění komplexní ochrany před škodlivým kódem. Jejímu nastavení a funkčnosti je proto potřeba věnovat zvýšenou pozornost. Pro zkontrolování dostupnosti aktualizace modulů klikněte v hlavním menu na záložku **Aktualizace** a následně na tlačítko **Zkontrolovat aktualizace**.

Pokud jste produkt dosud neaktivovali (například **licenčním klíčem**), budete k tomu vyzváni právě teď. Dokud nebude program aktivován, nebudou se stahovat aktualizace.



Další možnosti aktualizace naleznete v rozšířeném nastavení (dostupném v hlavním okně programu po kliknutí na možnost **Rozšířená nastavení** na záložce **Nastavení**, případně po stisknutí klávesy **F5**). Chcete-li nastavit pokročilé možnosti aktualizace, jako je režim aktualizace, přístup k serveru proxy a připojení LAN, přejděte do sekce **Aktualizace**.

- Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit**.



- Ve výchozím nastavení je v sekci **Profily** > **Aktualizace** > **Aktualizace modulů** aktivní možnost **Automatický výběr serveru**. Tím je zajištěna aktualizace produktu ze serverů ESET. Toto nastavení doporučujeme ponechat tak, jak je.
- Pokud nechcete zobrazovat bublinové upozornění v pravém dolním rohu obrazovky při úspěšné aktualizaci modulů, v sekci **Profily** > **Aktualizace** klikněte na **Změnit** na řádku **Konfigurace oznámení o událostech** a pomocí zaškrtávacích polí upravte hodnoty u položky **Detekční jádro bylo aktualizováno**.

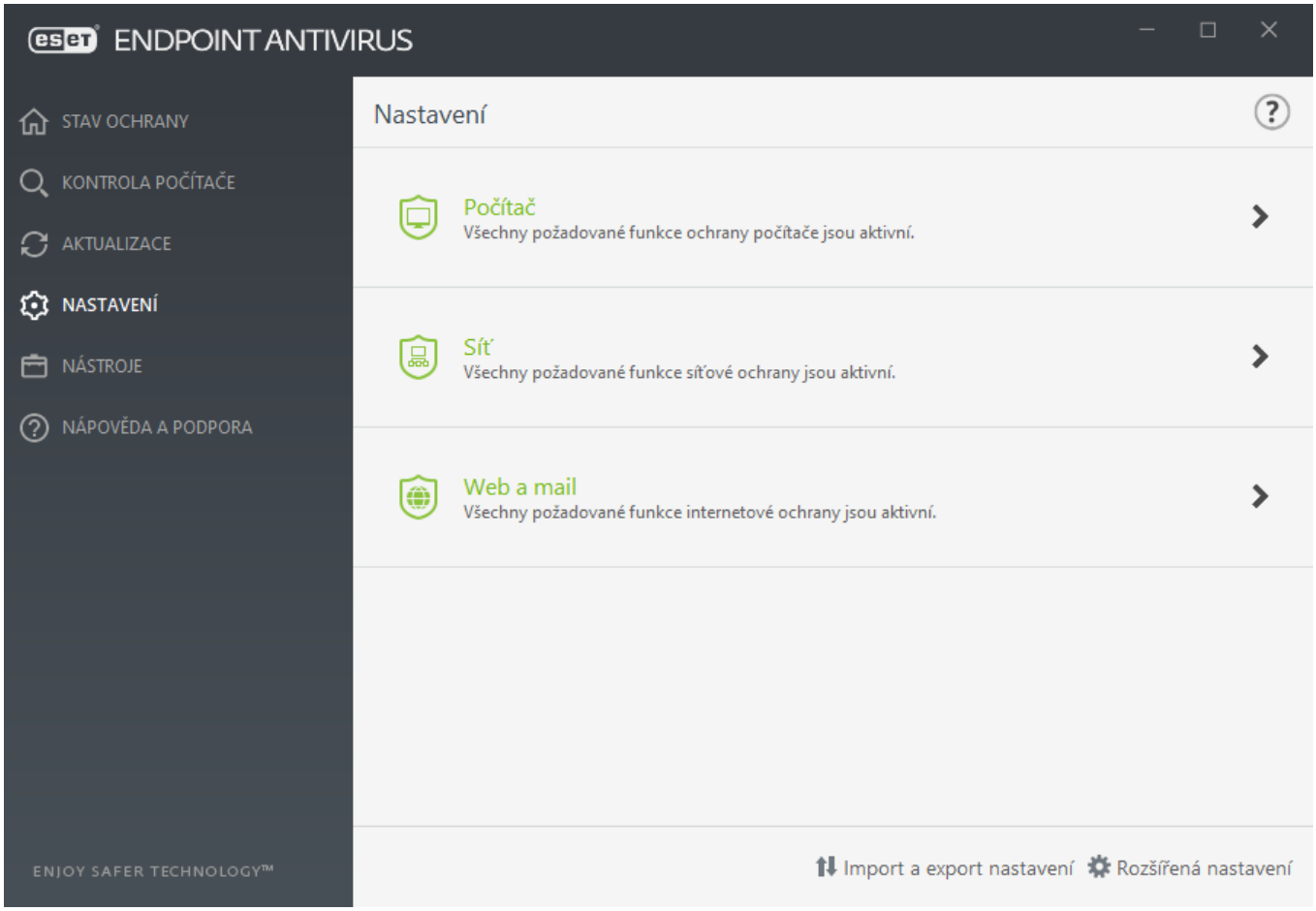
Pro zajištění optimální funkčnosti je nutné nechat program automaticky aktualizovat. To je možné pouze v případě, že zadáte platný **Licenční klíč** na záložce **Nápověda a podpora** > **Aktivovat produkt**.

Pokud nezadáte **Licenční klíč** po dokončení instalace, můžete jej zadat kdykoli poté. Více informací o aktivaci produktu naleznete v kapitole Jak aktivovat ESET Endpoint Antivirus.

Práce s ESET Endpoint Antivirus

V ESET Endpoint Antivirus můžete na záložce Nastavení konfigurovat úroveň ochrany počítače, stejně tak webové a poštovní ochrany.

> 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**

V sekci Počítač můžete zapnout nebo vypnout následující komponenty:

- **Rezidentní ochrana souborového systému** – všechny soubory jsou kontrolovány v momentu, kdy je vytvoříte, otevřete nebo spustíte.
- **Správa zařízení** – prostřednictvím tohoto modulu dokáže produkt omezit přístup k výměnným médiím (CD/DVD/USB/...). Přístup můžete omezit pouze pro čtení nebo úplně zakázat a pravidla lze aplikovat na konkrétního uživatele nebo celé skupiny uživatelů.
- **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). 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 a je plně funkční pouze s aktivní technologií ESET_LIVE_GRID. 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** – po aktivaci Prezentačního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. Zároveň hlavní okno změní barvu na oranžovou a upozorní vás na potenciální bezpečnostní riziko.

V sekci **Síť** můžete konfigurovat Ochranu proti síťovým útokům (IDS) a Ochranu proti zapojení do botnetu.

V sekci **Web a mail** můžete zapnout nebo vypnout následující moduly:

- **Ochrana přístupu na web** – pokud je zapnuta, veškerá komunikace přes HTTP nebo HTTPs je kontrolována na přítomnost škodlivého kódu,
- **Ochrana poštovních klientů** – zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím POP3 a IMAP protokolu,
- **Anti-Phishingová ochrana** – chrání vás před pokusy o získání hesel, bankovních dat a dalších důvěrných informací z webových stránek, které se tváří jako legitimní.

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tím dojde ke snížení úrovně ochrany počítače.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač pro znovu aktivování konkrétního modulu.

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 detailního nastavení konkrétního modulu klikněte na ozubené kolečko na řádku s názvem komponenty.

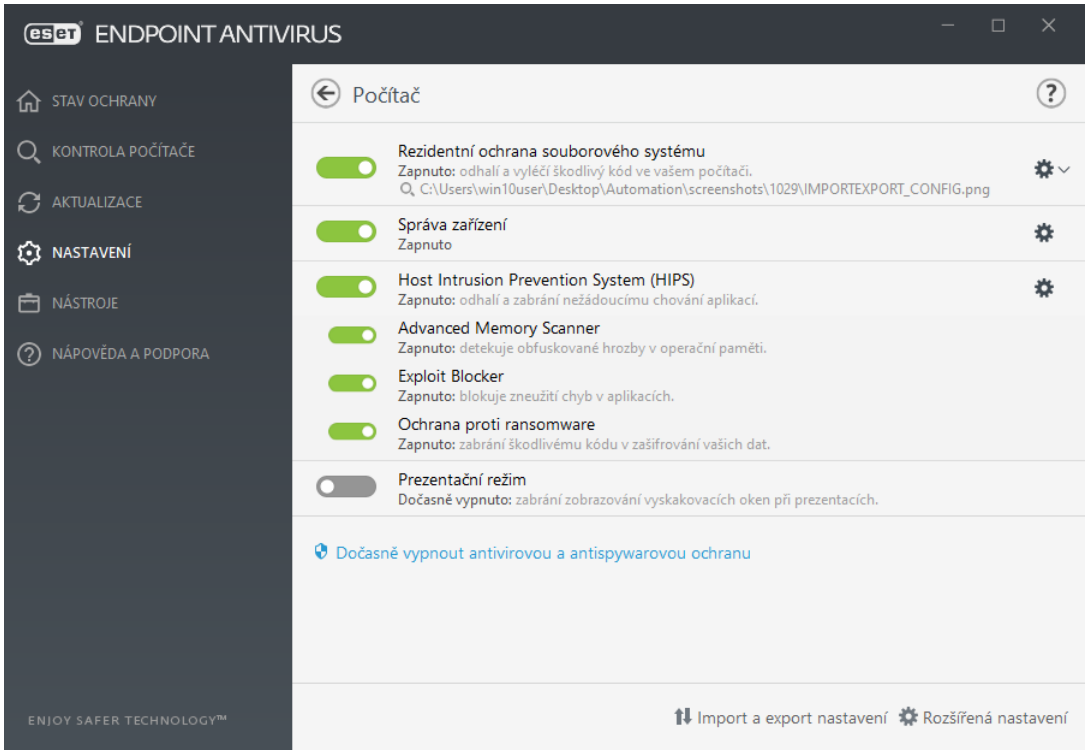
V dolní části obrazovky se nachází další možnosti související s konfigurací programu. Pro načtení již existující konfigurace z *.xml* konfiguračního souboru nebo pro uložení aktuálního nastavení do souboru klikněte na **Import a export nastavení**. Pro více informací přejděte do kapitoly Import a export nastavení.

Pokud chcete zobrazit detailní nastavení, klikněte na tlačítko **Rozšířená nastavení** nebo stiskněte klávesu **F5**.

Počítač

Jednotlivé moduly sekce **Počítač** naleznete po kliknutí na záložku **Nastavení** > **Počítač** v hlavním okně programu. Zobrazuje se zde stav ochrany jednotlivých modulů popsaných v předchozí kapitole. V této sekci jsou k dispozici následující nastavení:

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 a složky z kontroly. Pro zobrazení a **konfiguraci detailních parametrů** rezidentní ochrany vyberte možnost **Nastavit**.



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,
- **Správa zařízení** – prostřednictvím tohoto modulu dokáže produkt omezit přístup k výměnným médiím (CD/DVD/USB/...). Přístup můžete omezit pouze pro čtení nebo úplně zakázat a pravidla lze aplikovat na konkrétního uživatele nebo celé skupiny uživatelů.
- **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). 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 a je plně funkční pouze s aktivní technologií ESET_LIVE_GRID. 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** – po aktivaci Prezentačního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. 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**.

Detekční jádro

Detekční jádro chrání systém před škodlivými útoky tím, že kontroluje soubory, e-maily a internetovou komunikaci. Pokud detekuje objekt klasifikovaný jako malware, zahájí akci pro vyřešení situace. Detekční jádro může eliminovat objekt jeho zablokováním a následným vyléčením, odstraněním nebo přesunutím do karantény.

Pro konfiguraci detekčního jádra klikněte na tlačítko **Rozšířená nastavení** nebo stiskněte klávesu **F5**.

V této kapitole naleznete:

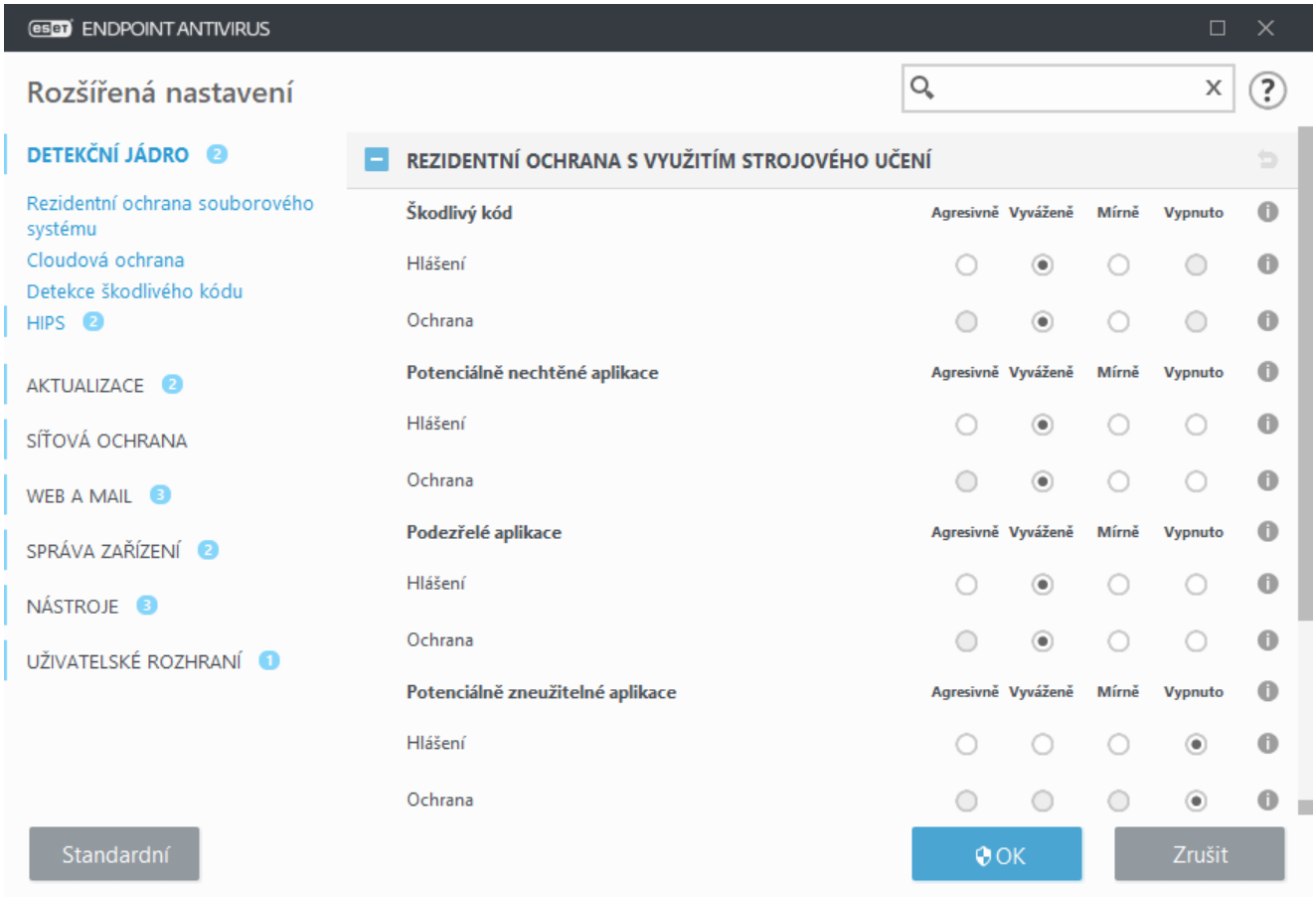
- Rezidentní ochrana s využitím strojového učení
- Detekce škodlivého kódu
- Nastavení hlášení
- Nastavení ochrany
- Best practices

> Od verze 7.2 již v nastavení detekčního jádra nejsou dostupné přepínače pro ZAPNUTÍ/VYPNUTÍ jako tomu bylo do verze 7.1. Nově si nastavujete práh ochrany, kdy si vyberte jeden z následujících způsobů detekce – "Agresivně", "Vyváženě", "Mírně" a "Vypnuto".

Rezidentní ochrana s využitím strojového učení

Nastavení možností v části **Rezidentní ochrana s využitím strojového učení** je platné pro všechny moduly ochrany (například rezidentní ochranu souborového systému, ochranu přístupu na web…). Nastavením definujete úroveň hlášení a ochrany pro následující kategorie detekcí:

- **Malware** – počítačový virus je škodlivý kód připojený k existujícímu souboru (na začátek nebo na konec) ve vašem 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 – potenciálně nechtěné aplikace) představuje 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.
- **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.
- **Podezřelé aplikace** jsou programy, které používají pro kompresi packery nebo jiné ochranné mechanismy zabraňující detekci. Tuto metodu často využívající tvůrci škodlivého kódu, aby se vyhnuli detekci ze strany antiviru.



Pokročilé strojové učení je nyní součástí detekčního jádra. Funguje jako pokročilá vrstva ochrany a vylepšuje detekci na základě strojového učení. Pro více informací o tomto typu ochranu se podívejte do slovníku pojmů.

Detekce škodlivého kódu

Nastavení skeneru může být odlišné pro rezidentní ochranu a **volitelnou kontrolu** počítače. Standardně je však aktivní možnost Použít nastavení rezidentní ochrany. To znamená, že se použije nastavení ze sekce **Detekční jádro** > **Rezidentní ochrana s využitím strojového učení**.

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 Antivirus povoleno).

Práh (úroveň) hlášení můžete konfigurovat jednotlivě pro každou kategorii (dále jen "KATEGORIE"):

1. Škodlivý kód

2. Potenciálně nechtěné aplikace
3. Potenciálně zneužitelné aplikace
4. Podezřelé aplikace

Vybraný práh pro hlášení přebírá detekční jádro Hlášení provádí 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 Antivirus

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

* Dostupná v ESET Endpoint Antivirus 7.2 a novějším
** Nedoporučeno.

⊟ Jak zjistím verzi produktu, programových modulů a data sestavení?

1. V hlavním okně programu klikněte na **Nápověda a podpora** > **O programu ESET Endpoint Antivirus**.
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 **Zobrazit moduly**.

Důležité poznámky

Při konfiguraci vhodných prahů ve svém prostředí vezměte v potaz následující informace:

- Možnost **Vyváženě** je doporučená pro většinu situací.
- Možnost **Mírně** představuje srovnatelnou úroveň ochrany, která byla dostupná v předchozích verzích ESET Endpoint Antivirus (7.1 a starších). Toto nastavení je doporučené 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 Antivirus 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.

Konverze ESET PROTECT politik pro ESET Endpoint Antivirus 7.1 a starší

V konfiguračním editoru ESET PROTECT již nejsou v nastavení skeneru u jednotlivých KATEGORIÍ dostupné přepínače pro ZAPNUTÍ/VYPNUTÍ. Níže naleznete konverzní matici nově představených prahů ochrany na stavy přepínačů dostupné v produktu ESET Endpoint Antivirus ve verzi 7.1 a starším.

Práh pro KATEGORII	Agresivně	Vyváženě	Mírně	Vypnuto
Použitý přepínač pro KATEGORII	✓	✓	✓	✗

Po aktualizaci produktu z verze 7.1 na verzi 7.2 a novější se nastavení změní následovně:

Stav přepínače KATEGORIE před aktualizací	✓	✗
Práh KATEGORIE po aktualizaci	Vyváženě	Vypnuto

Best practices

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 Antivirus.
- **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.

Rozšířená nastavení detekčního jádra

Technologie Anti-Stealth je sofistikovaný systém pro detekci nebezpečných programů například rootkitů, které jsou po svém spuštění neviditelné pro operační systém. Ty jsou imunní vůči standardním detekčním technikám.

Zapnout rozšířenou kontrolu prostřednictvím AMSI – nástroj Microsoft Antimalware Scan Interface poskytuje vývojářům aplikací nové možnosti ochrany před škodlivým kódem (tato funkce je dostupná ve Windows 10 a 11).

Nalezena infiltrace

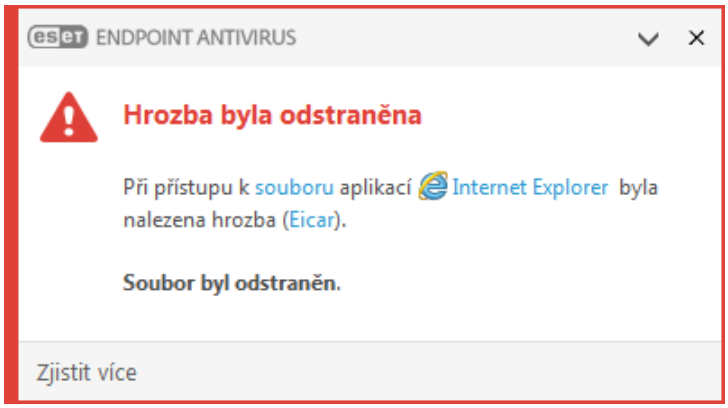
Infiltrace se mohou do počítače dostat z různých zdrojů: z webových stránek, ze sdílených složek, prostřednictvím e-mailu, z výměnných médií (USB, externí disků, CD a DVD jiných).

Standardní chování

ESET Endpoint Antivirus dokáže zachytit infiltrace pomocí:

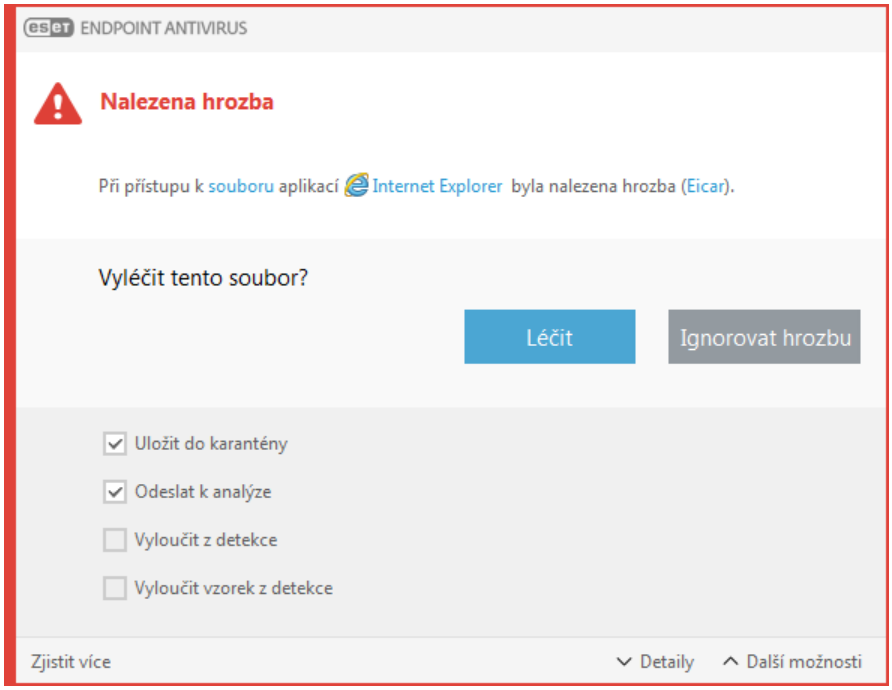
- Rezidentní ochrany souborového systému,
- Ochrana přístupu na web
- Ochrany poštovních klientů,
- Volitelné kontroly počítače.

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 Antivirus 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.

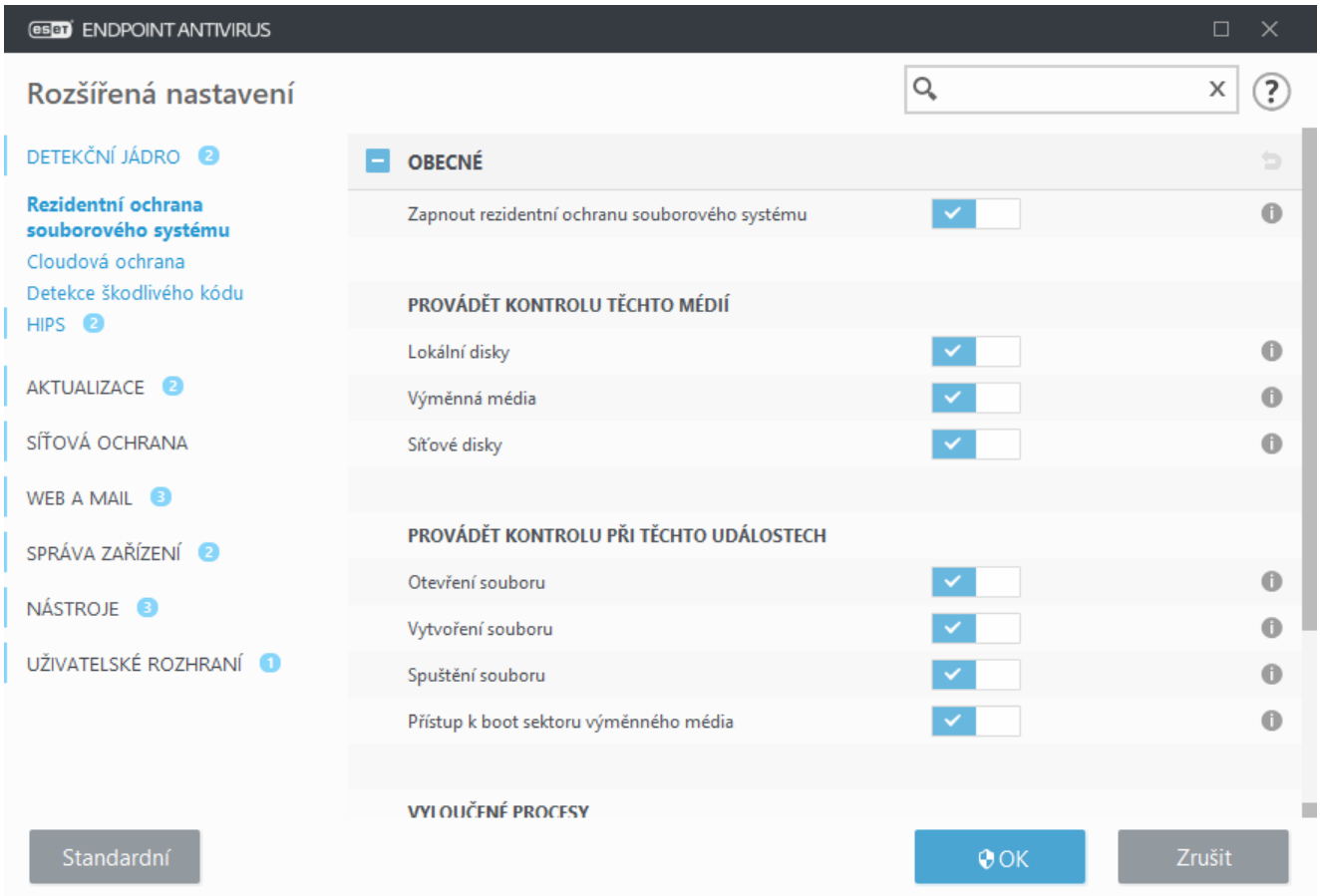
Pokud se váš počítač chová podezřele nebo máte podezření, že je infikován (zamrzá, je pomalý atp.), postupujte podle následujících kroků:

- Otevřete hlavní okno programu ESET Endpoint Antivirus 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.

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** > **Detekční jádro** > **Rezidentní ochrana souborového systému** > **Obecné**.

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 soubory kontrolovány při otevírání, spouštění a vytváření. 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 vložené výměnné médium obsahuje boot sektor, po aktivování této možnosti dojde automaticky k jeho zkontrolování po připojení zařízení. Tato možnost nezapíná kontrolu souborů na výměnných médiích. Nastavení kontroly na výměnných médiích se nachází v části **Provádět kontrolu těchto médií** > **Výměnná média**. Pro správné fungování **kontroly boot sektoru výměnných médií** ponechte v sekci parametry skenovacího jádra ThreatSense aktivní možnost **Boot sektory/UEFI**.

Procesy vyloučené z kontroly – více informací o tomto typu výjimek naleznete v kapitole Vyloučené procesy.

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 může být odlišné u nově vytvářených než existujících souborů. 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. Pokud chcete možnosti kontroly upravit, přejděte v **Rozšířeném nastavení** (dostupném po stisknutím klávesy **F5** v hlavním okně programu) do sekce **Detekční jádro** > Rezidentní ochrana souborového systému. Dále přejděte na záložku **Parametry skenovacího jádra ThreatSense** > **Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

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.

Kdy měnit nastavení rezidentní ochrany

Proto je potřeba být při změnách nastavení obezřetný. Proto je potřeba být při změnách nastavení obezřetný. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech.

Po instalaci ESET Endpoint Antivirus jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Pro obnovení nastavení na standardní hodnoty klikněte na šipku , která se nachází v pravé části okna **Rozšířená nastavení** > **Detekční jádro** > **Rezidentní ochrana souborového systému**.

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. Opětovné zapnutí je možné v hlavním okně programu na záložce **Nastavení** po kliknutí na **Ochrana počítače** > **Rezidentní ochrana souborového systému**.

Pokud se rezidentní ochrana nespouští při startu operačního systému, pravděpodobně byla vypnuta možnost **Zapnout rezidentní ochranu souborového systému**. Pro ujištění, zda je možnost zapnutá, přejděte do **Rozšířeného nastavení** (dostupného po stisknutí klávesy **F5** v hlavním okně programu), následně na záložku **Detekční jádro** > **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

Ujistěte se, zda nemáte nainstalovaný další bezpečnostní program. Pokud jsou na zařízení nainstalované dva bezpečnostními programy, může mezi nimi docházet ke konfliktu. Proto doporučujeme před instalací produktu ESET všechny ostatní antivirové programy odinstalovat.

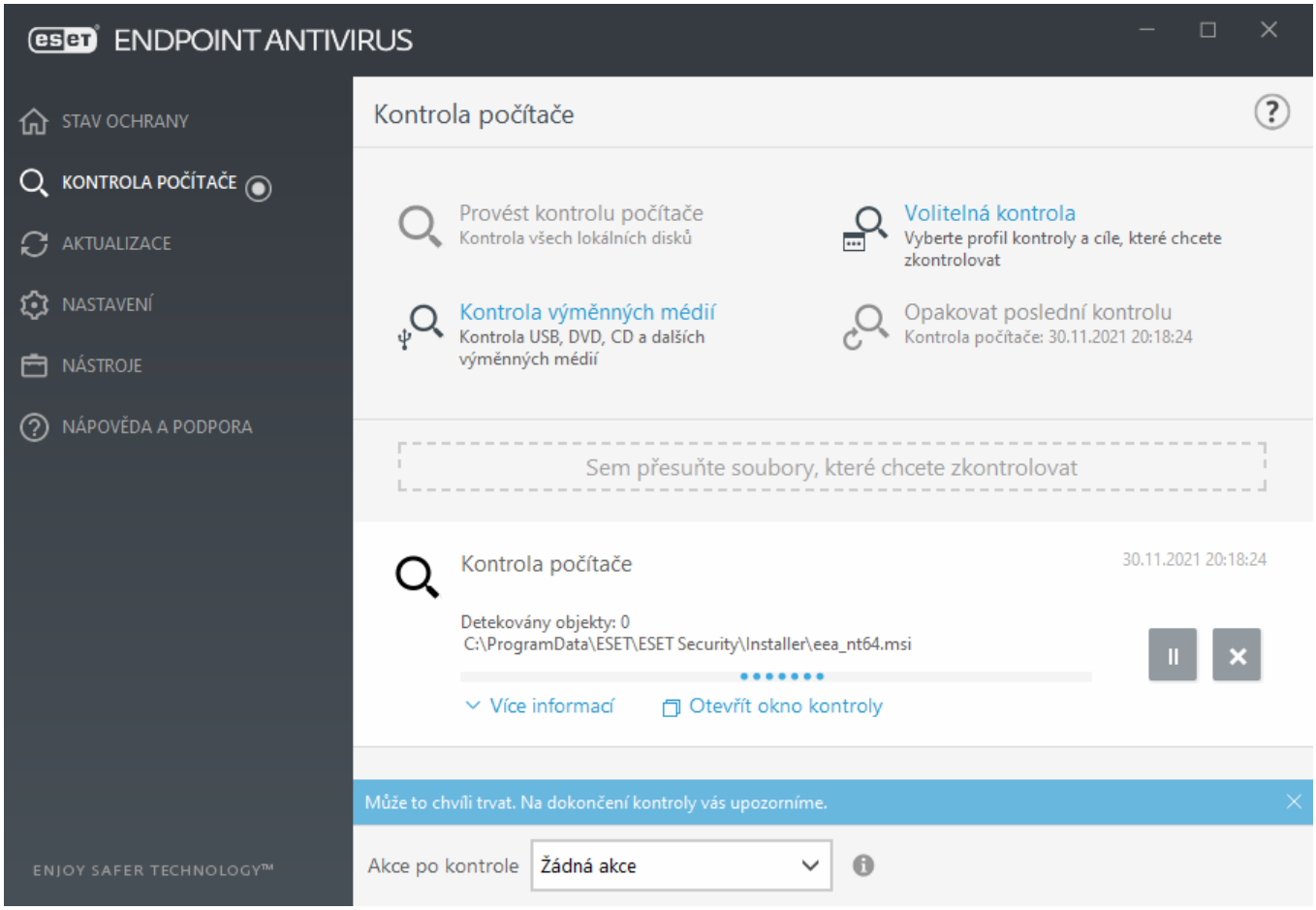
Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Zapnout rezidentní ochranu souborového systému**, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET. V takovém případě vytvořte ESET SysInspector protokol, který pomůže při diagnostice, a společně s popisem problému jej zašlete specialistům technické podpory. Další informace naleznete v článku ESET Databáze znalostí (článek nemusí být dostupný ve všech jazycích).

Kontrola počítače

Důležitou součástí antivirového ESET Endpoint Antivirus 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

Smart kontrola slouží pro rychlé spuštění kontroly počítače a automaticky léčí nebo odstraňuje infikované soubory a nevyžaduje interakci uživatele. Výhodou Smart kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. Smart kontrola zkontroluje všechny soubory na lokálních jednotkách a automaticky je vyléčí nebo odstraní. Úroveň léčení je nastavena na standardní úroveň. Více informací o typech léčení se dozvíte v kapitole Léčení.

Volitelná kontrola

Volitelná kontrola umožňuje výběr z předdefinovaných profilů kontroly a cílů kontroly. Výhodou volitelné kontroly je možnost podrobně specifikovat její parametry. Nastavenou konfiguraci můžete uložit do uživatelských profilů, které se dají využít při opakované kontrole.

Pro výběr cílů kontroly klikněte na **Kontrola počítače** > **Vlastní kontrola** a z rozbalovacího menu vyberte **Cíle kontroly** nebo je vyberte ručně ze stromové struktury. Cíle kontroly můžete definovat také přímým zadáním cesty k souboru nebo složce. Pokud chcete spustit pouze kontroly systému, a neléčit případné infiltrace, zaškrtněte možnost **Zkontrolovat bez léčení**. K dispozici jsou tři úrovně léčení, které můžete definovat po kliknutí na **Nastavit**

> **Parametry skenovacího jádra ThreatSense** > **Léčení**.

Provádění volitelné kontroly s vlastními parametry je určeno pokročilým uživatelům, kteří již mají zkušenosti s používáním antivirových programů.

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

Kontrola výměnných médií

Funguje podobně jako možnost **Provést kontrolu počítače** – spustí rychlou kontrolu výměnných médií (CD/DVD/USB), která jsou aktuálně připojené k počítači. To může být užitečné ve chvíli, kdy si přeje zkontrolovat obsah připojeného USB zařízení k počítači na škodlivý software 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.

Z rozbalovací nabídky **Akce po kontrole** si vyberte jednu z dostupných možností: **Žádná akce**, **Vypnout**, **Restartovat**, **Restartovat v případě potřeby**, **V případě potřeby vynutit restart** nebo **Vynutit restart**. Akce **Režim spánku** nebo **Hibernace** je dostupná na základě Nastavení napájení a režimu spánku, případně možnostech vašeho zařízení. Vybraná akce se provede po dokončení všech běžících kontrol. Pokud je vybrána možnost **Vypnout**, zobrazí se potvrzovací dialogové okno s 30sekundovým odpočtem (kliknutím na tlačítko **Zrušit** vypnutí přerušíte). Další informace naleznete v kapitole Rozšířená nastavení kontroly.

> 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 nechcete kontrolovat celý disk, ale pouze specifickou oblast, vyberte možnost Volitelná kontrola kliknutím v hlavním okně na záložku **Kontrola počítače** > **Volitelná kontrola** a pro výběr cílů kontroly využijte stromovou strukturu nebo klikněte na ozubené kolečko a použijte rozbalovací menu **Cíle kontroly**.

Prostřednictvím cílů kontroly můžete vybrat objekty (operační paměť, jednotky, sektory, soubory a složky), které chcete zkontrolovat na přítomnost hrozeb.

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

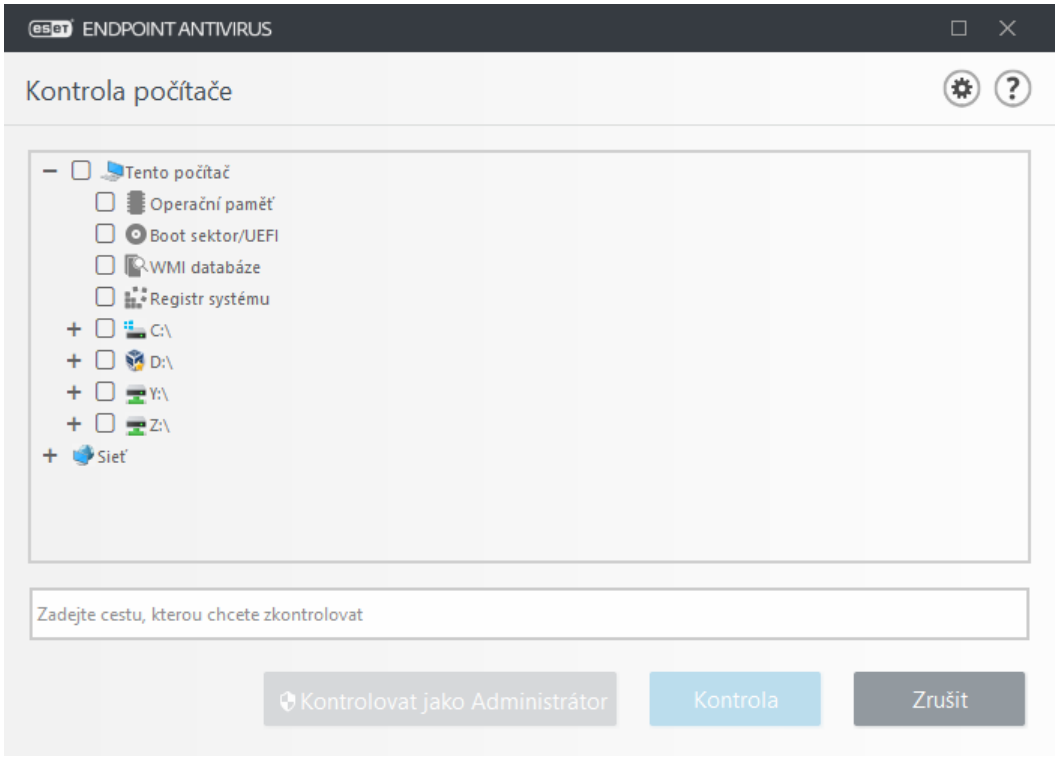
- **Podle nastavení profilu** – vybere cíle nastavené ve vybraném profilu kontroly.
- **Výměnné disky** – vybere diskety, USB flash disky, CD/DVD.
- **Lokální disky** – vybere lokální pevné disky v počítači.
- **Síťové disky** – vybere namapované síťové disky.

- **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.



Infikované soubory nejsou léčeny automaticky. Kontrolou bez léčení můžete získat přehled o aktuálním stavu bezpečnosti počítače. V **rozšířeném nastavení** v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** si v části **Parametry skenovacího jádra ThreatSense** můžete pomocí rozbalovacího menu vybrat jednu ze tří úrovní **Léčení**. Pokud chcete spustit pouze kontroly systému, a neléčit případné infiltrace, zaškrtněte možnost **Zkontrolovat bez léčení**. Historie kontrol je zaznamenána do protokolu kontrol.

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

Pro kontrolu můžete použít předdefinované profily v rozbalovacím menu **Profil kontroly**. Výchozím profilem je **Smart kontrola počítače**. Dále jsou dostupné dva předdefinované profily pojmenované **Hloubková kontrola počítače** a **Kontrola z kontextového menu**. Navzájem se liší odlišným nastavením parametrů skenovacího jádra ThreatSense. Profily kontroly můžete definovat v **Rozšířeném nastavení** v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** > Seznam profilů (a následně nastavit rozdílně parametry skenování jádra

ThreatSense.

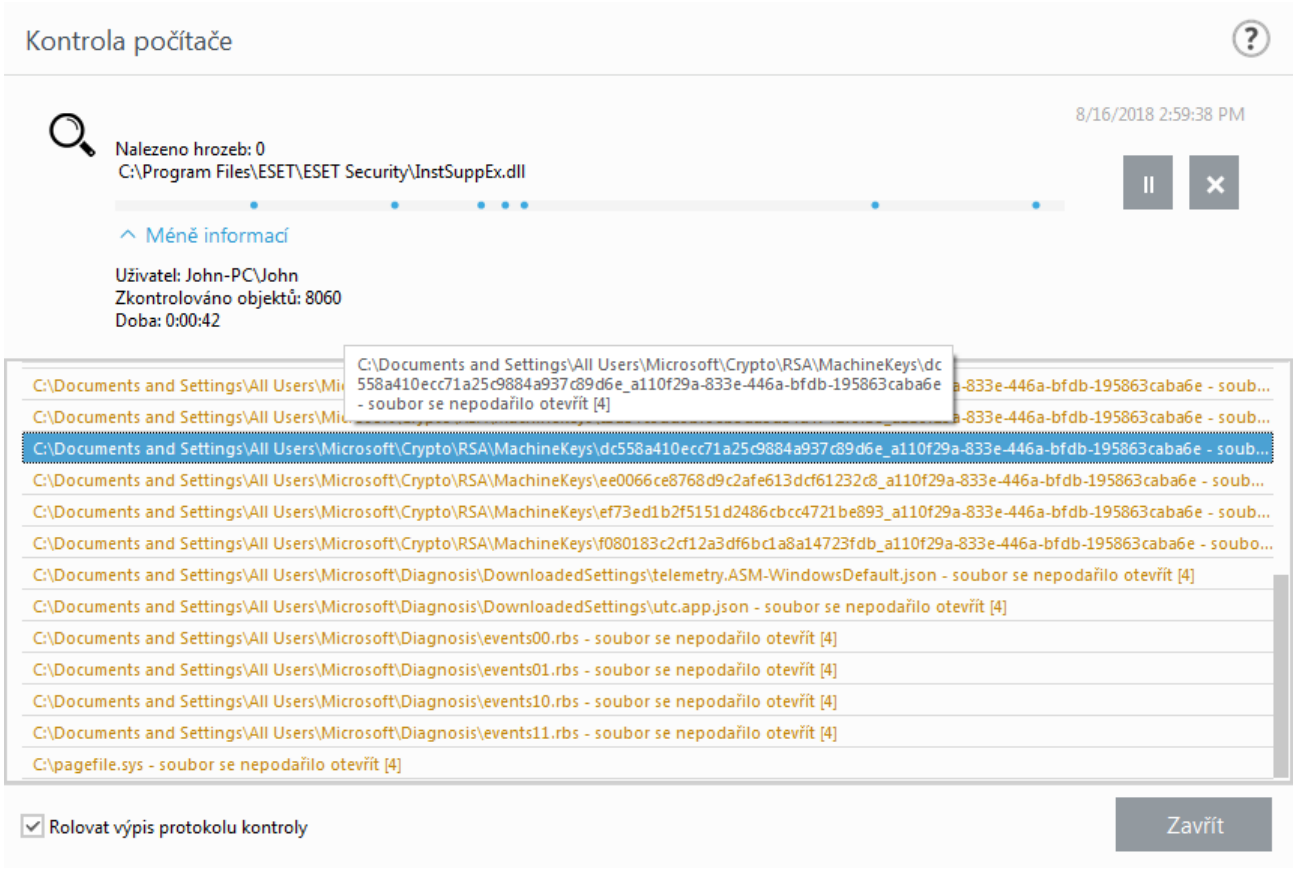
Kliknutím na tlačítko **Kontrolovat** spustíte kontrolu počítače s nastavenými parametry.

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 v pořádku, pokud určité typy souborů jako například zaheslovaná data nebo soubory využívané operačním systémem (například *pagefile.sys* a některé soubory protokolů) nemohou být zkontrolovány.

Průběh kontroly – grafická reprezentace vyjádření poměru již zkontrolovaných souborů k celkovému množství souborů, které se mají kontrolovat. Rychlost kontrolního procesu je odvozena od celkového počtu objektů zahrnutých do kontroly.

Cíl – název právě kontrolovaného souboru a jeho umístění.

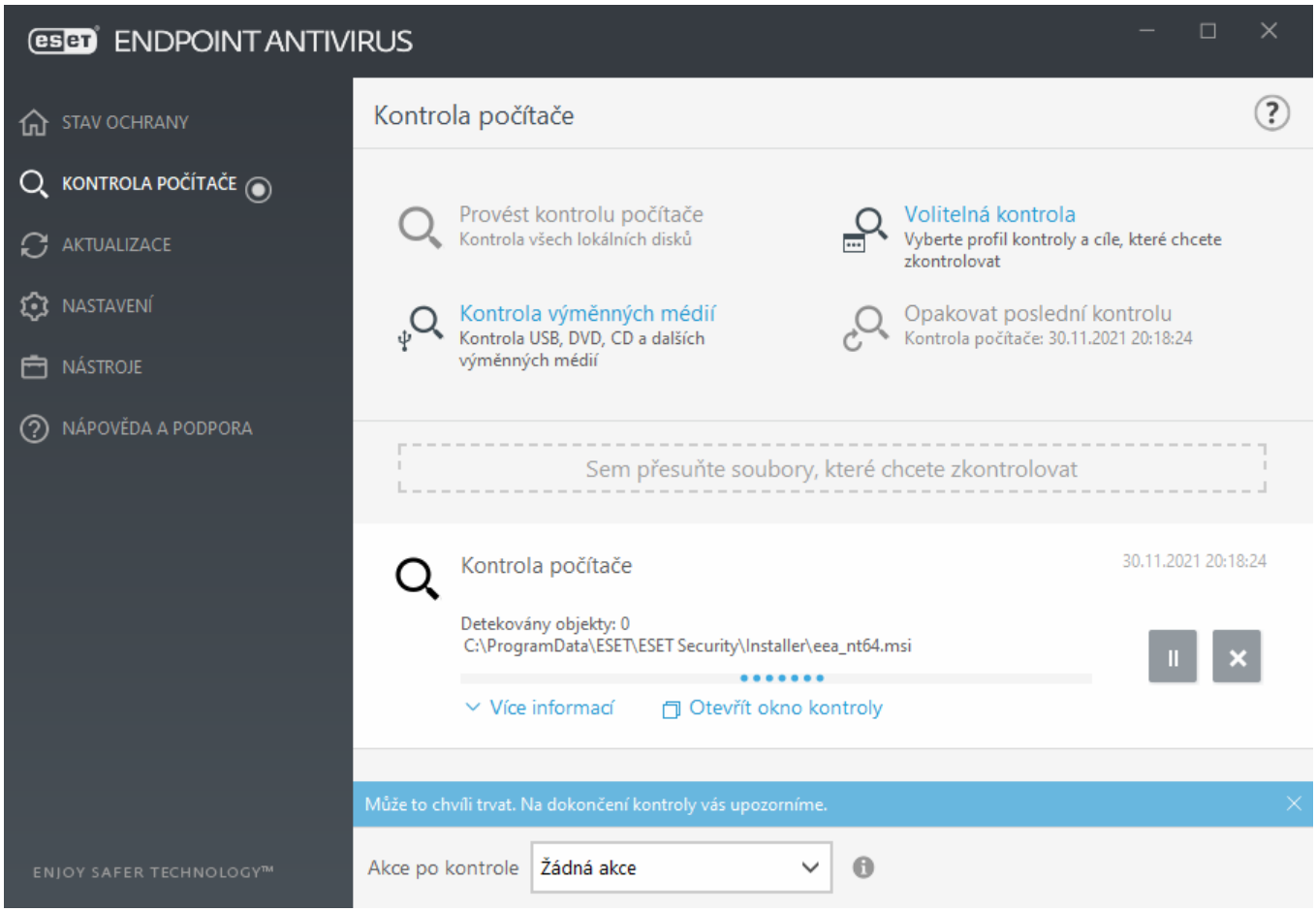
Nalezeno hrozeb – celkový počet nalezených hrozeb v průběhu aktuální kontroly.

Pauza – pozastaví právě probíhající kontrolu.

Pokračovat – možnost se zobrazí po pozastavení kontroly. Opětovným kliknutím na **tlačítko** bude kontrola pokračovat.

Zastavit – ukončí právě probíhající kontrolu.

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



Protokol kontroly počítače

V protokolu kontroly počítače jsou uvedeny obecné informace následujícího typu:

- Datum a čas kontroly
- Kontrolované disky, složky a soubory
- Počet zkontrolovaných objektů
- Počet nalezených hrozeb
- Čas dokončení
- Doba kontroly

Detekce škodlivého kódu

Možnosti pro konfiguraci parametrů **detekce škodlivého kódu** při volitelné kontrole počítače naleznete v Rozšířeném nastavení. V hlavním okně programu stiskněte klávesu **F5** a přejděte do sekce **Detekční jádro** > **Detekce škodlivého kódu** a nastavte si parametry kontroly. K dispozici jsou následující možnosti:

- **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. Pro více informací o přejděte do kapitoly Profily kontroly.
- **Volitelná ochrana s využitím strojového učení** – více informací naleznete v kapitole Detekční jádro (ve verzi 7.2 a novější).
- **Cíle kontroly** – pokud chcete kontrolovat pouze konkrétní cíl, můžete po kliknutí na tlačítko **Změnit** na řádku **Cíle kontroly** definovat cíle výběrem ze stromové struktury nebo ručním zadání cesty k souborům/složkám. Více naleznete v kapitole Cíle kontroly.
- Parametry skenovacího jádra **ThreatSense** – detailnější nastavení kontroly, jako např. typy souborů, které si přejete kontrolovat, metody detekce a jiné. Dostupné možnosti zobrazíte po kliknutí na tuto záložku.

Kontrola při nečinnosti

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

Kontrola při nečinnosti

Funkci **aktivujete** pomocí přepínače **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 změnit zaškrtnutím možnosti **Spustit také při napájení počítače z baterie** v Rozšířeném nastavení.

Vyberte možnost **Zapisovat do protokolu**, pokud chcete průběh kontroly zapisovat do protokolu a mít k výsledkům přístup v hlavním okně programu na záložce **Nástroje** > **Protokoly** > **Kontrola počítače**.

Detekce stavu nečinnosti

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

Pro úpravu parametrů prováděné kontroly (například režimu detekce, úrovně léčení atp.) přejděte do sekce parametry skenovacího jádra ThreatSense.

Profily kontroly

K dispozici jsou čtyři předdefinované profily kontroly ESET Endpoint Antivirus:

- **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 **Rozšířené nastavení** (dostupné po stisknutí klávesy F5 v hlavním okně programu), přejděte na záložku **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola**. Kliknutím na **Změnit** na řádku **Seznam profilů** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. V kapitole parametry skenovacího jádra ThreatSense naleznete popis jednotlivých parametrů pro nastavení kontroly počítače.

> Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy nebo potenciálně nebezpečné aplikace a přitom požadujete **Přísné léčení**? 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 cílů kontroly můžete vybrat objekty (operační paměť, jednotky, sektory, soubory a složky), které chcete zkontrolovat na přítomnost hrozeb.

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.

Rozšířená nastavení kontroly

V tomto okně můžete konfigurovat detaily naplánované úlohy kontroly počítače. Z rozbalovacího menu můžete vybrat akci, která se má provést po dokončení kontroly:

- **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 vyžadováno,
- **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.
- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.

> 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 **Akci 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.

Pro více informací se podívejte do kapitoly Průběh kontroly.

Správa zařízení

Prostřednictvím tohoto modulu dokáže ESET Endpoint Antivirus omezit přístup k výměnných médií (CD/DVD/USB/…). Přístup můžete omezit pouze pro čtení nebo úplně zakázat a pravidla lze aplikovat na konkrétního uživatele nebo celé skupiny uživatelů. Tuto funkci můžete použít v případě, kdy chcete uživatelům například zabránit připojování výměnných médií k počítači.

Podporovaná externí zařízení:

- Datové úložiště (HDD, USB výměnné jednotky),
- CD/DVD
- USB tiskárna,
- FireWire úložiště,
- Bluetooth zařízení,
- 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** (dostupném po stisknutí klávesy F5 v hlavním okně programu) > **Správa zařízení**.

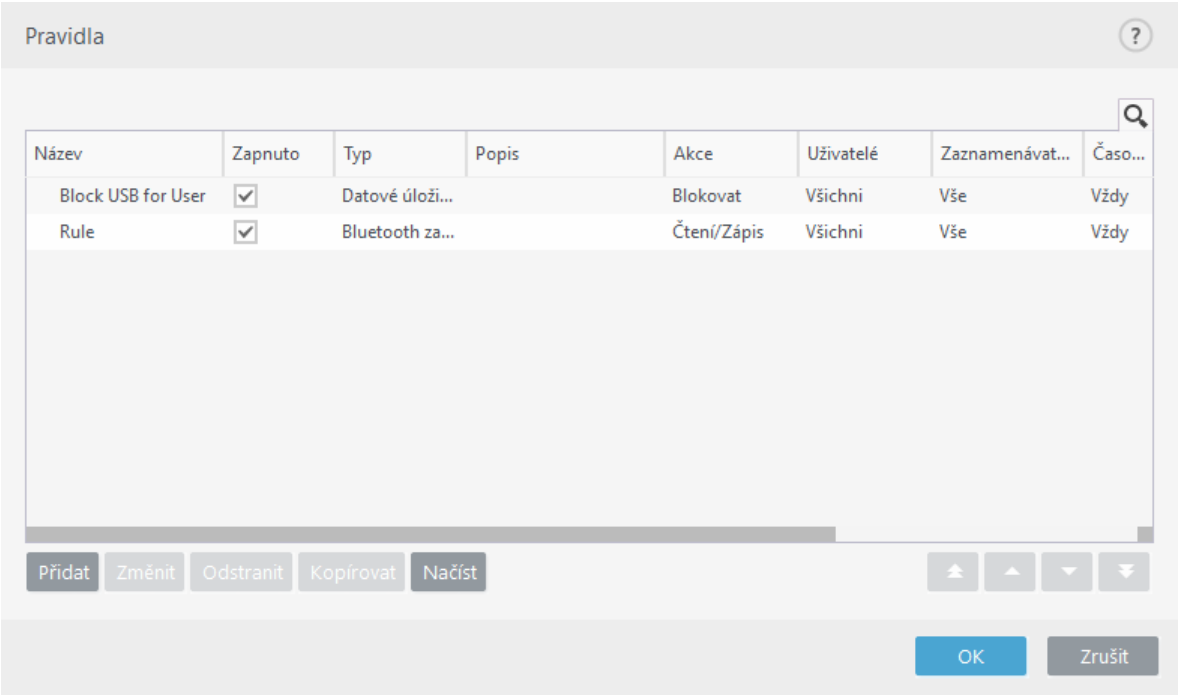
Kliknutím na přepínač **Zapnout správu zařízení** aktivujete funkci Správa zařízení v produktu ESET Endpoint Antivirus. Pro provedení změn bude potřeba restartovat počítač. Po aktivaci funkce se zpřístupní odkaz **Pravidla**, prostřednictvím kterého si otevřete editor pravidel.

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 Antivirus 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).

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.

Změnit – umožní změnit skupinu zařízení a parametry zařízení.

Odstranit – vymaže vybranou skupinu nebo konkrétní zařízení.

Importovat – pomocí této možnosti importujte seznam zařízení z textového souboru. Soubor musí splňovat následující formát:

- Každé zařízení musí být uvedeno na novém 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).

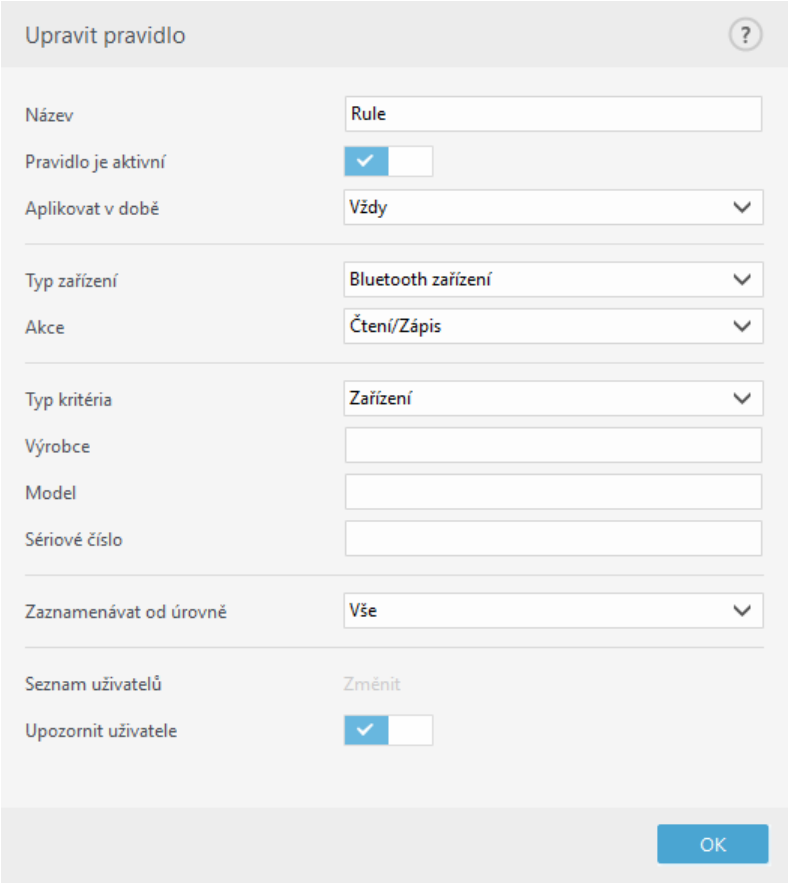
Po dokončení konfigurace klikněte na tlačítko **OK**. Klikněte na tlačítko **Zrušit** pro zavření dialogového okna bez uložení změn.

> Na každou vytvořenou skupinu zařízení můžete aplikovat rozdílná pravidla. Dále můžete vytvořit jednu skupinu, které nastavíte akci **Blokovat**. Poté vytvořte druhé pravidlo, které bude blokovat přístup.

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 **Pouze pro čtení** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

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. Zaškrtnutím možnosti **Pravidlo je aktivní** dané pravidlo povolíte. Pokud ponecháte tuto možnost neaktivní, pravidlo se nebude uplatňovat a můžete jej použít v budoucnu.

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. Pro více informací přejděte do kapitoly 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:

- **Čtení/Zápis** – plný přístup k zařízení,
- **Blokovat** – přístup k zařízení bude zakázán,
- **Pouze pro čtení** – uživatel může pouze číst soubory na daném zařízení,
- **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 **Pouze pro čtení** 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:

- **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. Filtrování parametrů rozlišuje velikost písmen a nepodporuje zástupné znaky (*, ?).

> 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.

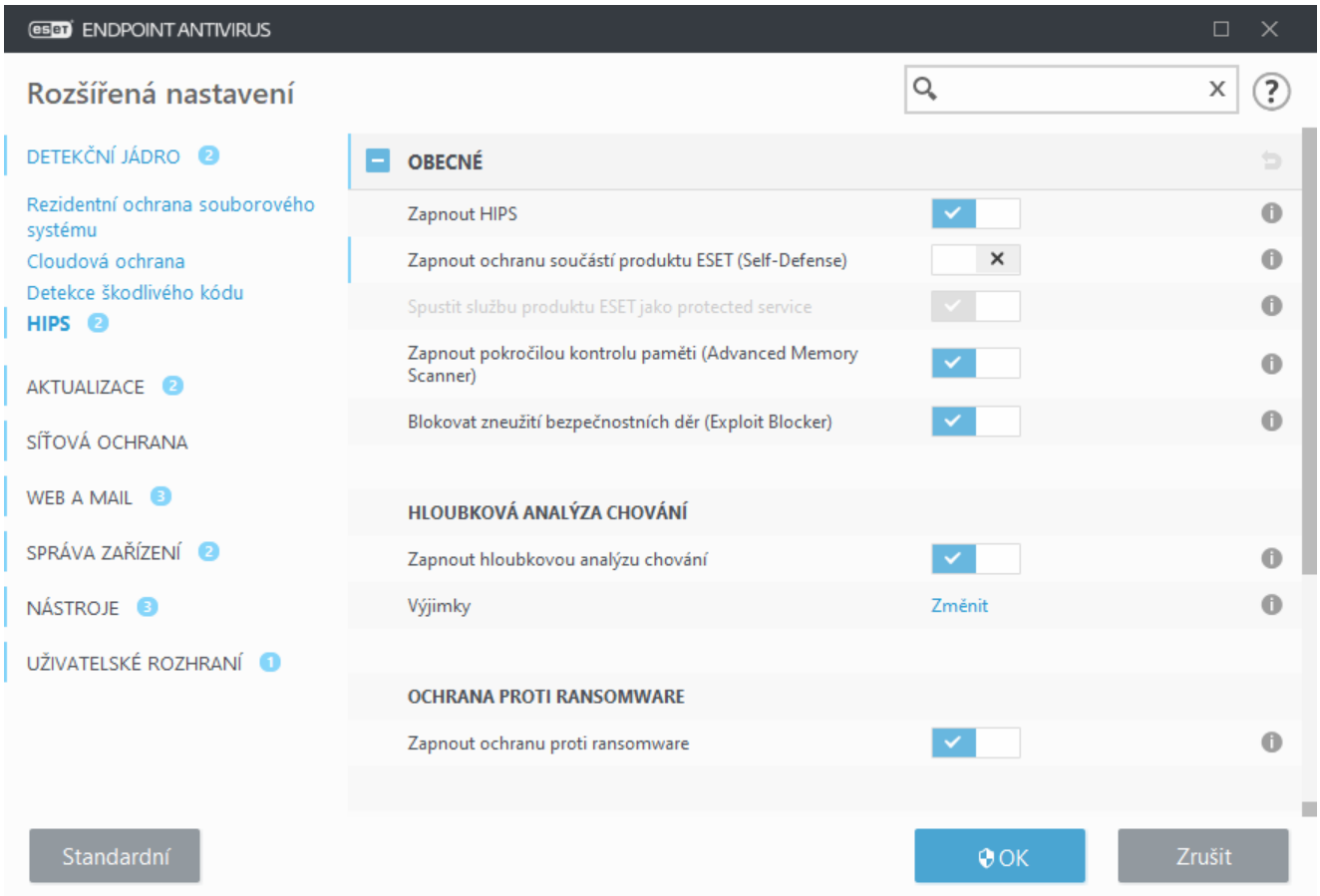
Mějte na paměti, že není možné omezit všechna zařízení. Například zobrazovací zařízení neposkytují žádné informace o uživateli, pouze vyvolávají akci.

Host-based Intrusion Prevention System (HIPS)

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.

Nastavení HIPS naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5) v sekci **Detekční jádro** > **HIPS** > **Obecné**. Stav ochrany HIPS je zobrazen v hlavním okně ESET Endpoint Antivirus na záložce **Nastavení** v sekci **Počítač**.



Obecné

Zapnout HIPS – HIPS je v ESET Endpoint Antivirus standardně zapnutý. Jeho vypnutím zakážete běh dalších součástí HIPS jako je například Exploit Blocker.

Zapnout ochranu součástí produktu ESET (Self-Defense) – ESET Endpoint Antivirus 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). 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 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 Antivirus. 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.

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.

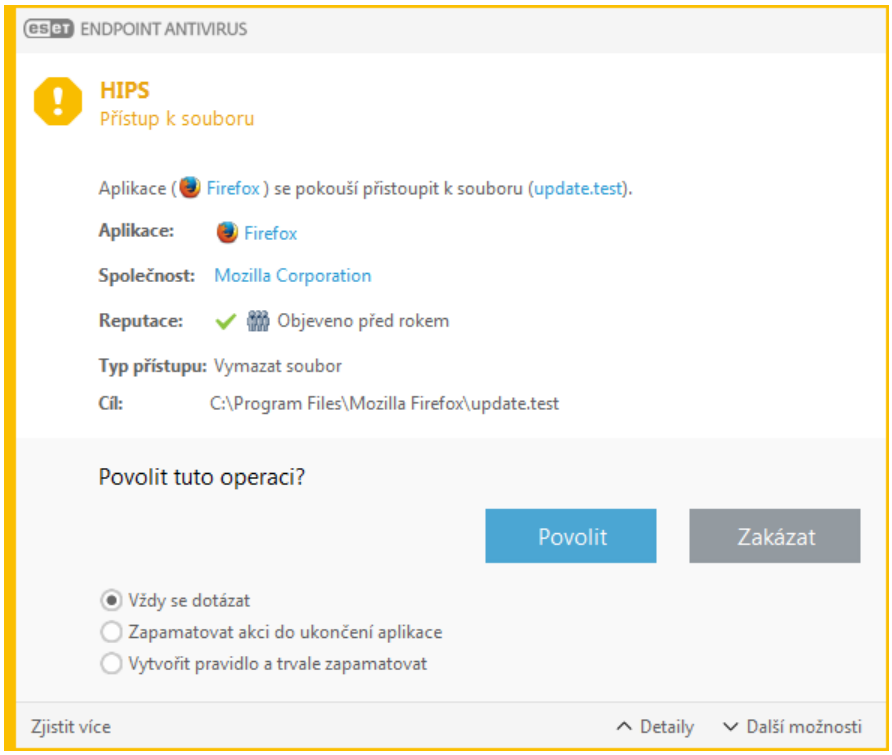
Vybráním možnosti **Vytvořit pravidlo a trvale zapamatovat** vytvoříte nové HIPS pravidlo, kterém můžete následně modifikovat prostřednictvím Editoru HIPS pravidel (ke změně pravidel je vyžadováno oprávnění administrátora).

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** (dostupném po stisknutí klávesy F5 v hlavním okně programu) 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**.

Po kliknutí na možnost **Detaily** si zobrazíte konkrétní **detekční parametry.** Prostřednictvím tohoto dialogového okna můžete **odeslat vzorek do virové laboratoře k bližší analýze**, případně danou aplikaci **vyloučit z 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.

Upozornit uživatele – 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

V této části nejsou dostupná tlačítka (nahoru/dolů) pro ovlivnění priority pravidel HIPS.

- 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 – odškrtněte tuto možnost, pokud chcete ponechat pravidlo v seznamu pravidel a nepoužívat ho.

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do protokolu HIPS.

Upozornit uživatele – při výskytu události se v pravém dolním rohu obrazovky zobrazí 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.

Některé operace není možné monitorovat na 64bitové verzi Windows XP.

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.

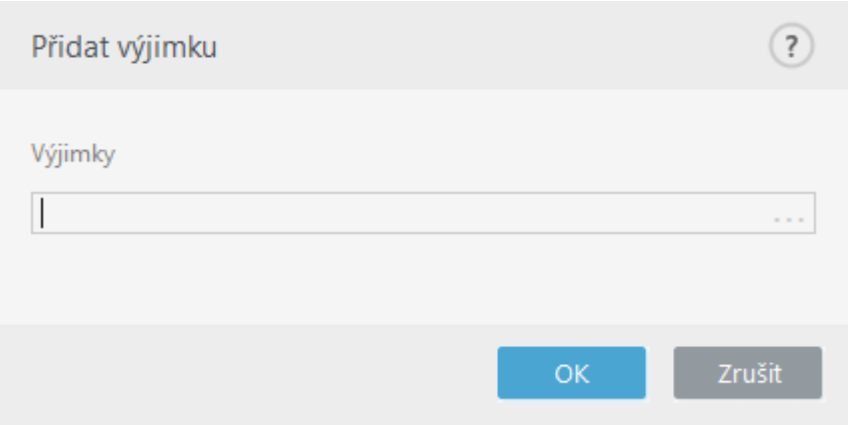
Použití zástupných znaků v pravidlech
Hvězdičku můžete v pravidlech použít pouze jako náhradu konkrétního klíče, například "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start". Ostatní možnosti použití zástupných znaků nejsou podporovány.

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**.



Rozšířená nastavení HIPS

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

Automaticky povolené ovladače – vybrané ovladače 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.

Prezentační režim

Prezentační režim je funkce pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru. 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 na záložce **Nastavení** > **Počítač**. V **Rozšířeném nastavením** (dostupném po stisknutí **klávesy F5**) můžete v sekci **Nástroje** > **Prezentační režim** aktivovat možnost **Automaticky zapnout Prezentační režim při běhu aplikací zobrazených na celou obrazovku**. Tím zajistíte, že ESET Endpoint Antivirus automaticky aktivuje Prezentační režim při spuštění aplikace v režimu celé obrazovky. 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**.

Vybráním možnosti **Automaticky zapnout Prezentační režim při zobrazení aplikací na celou obrazovku** se Prezentační režim automaticky zapne po spuštění aplikace na celou obrazovku a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování Prezentačního režimu po spuštění hry nebo zahájení prezentace.

Můžete také aktivovat možnost **Automaticky vypínat Prezentační režim** a následně definovat interval, po jehož uplynutí se Prezentační režim automaticky vypne.

Kontrola po startu

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

Možnosti nastavení kontroly po startu jsou součástí naplánované úlohy **Kontrola souborů spouštěných po startu**. Pro změnu tohoto nastavení klikněte v hlavním okně na záložku **Nástroje** > **Plánovač** > **Kontrola souborů spouštěných při startu** a následně na tlačítko **Změnit**. V posledním kroku se zobrazí okno Kontrola souborů spouštěných po startu počítače (pro více informací přejděte do další kapitoly).

Více informací o tvorbě a správě úloh Plánovače naleznete v kapitole Vytvoření nové úlohy.

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 spouštěné 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 klíči registru *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Seznamy souborů ke kontrole jsou pro každou skupinu pevně definovány.

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.

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** (dostupného po stisknutí klávesy **F5** v hlavním okně programu) a v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Ochrana dokumentů** klikněte na přepínač **Zapnout ochranu dokumentů**.

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).

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 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.

Ve verzi 7.1 a starších byla konfigurace výkonnostních a detekčních výjimek společná.

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

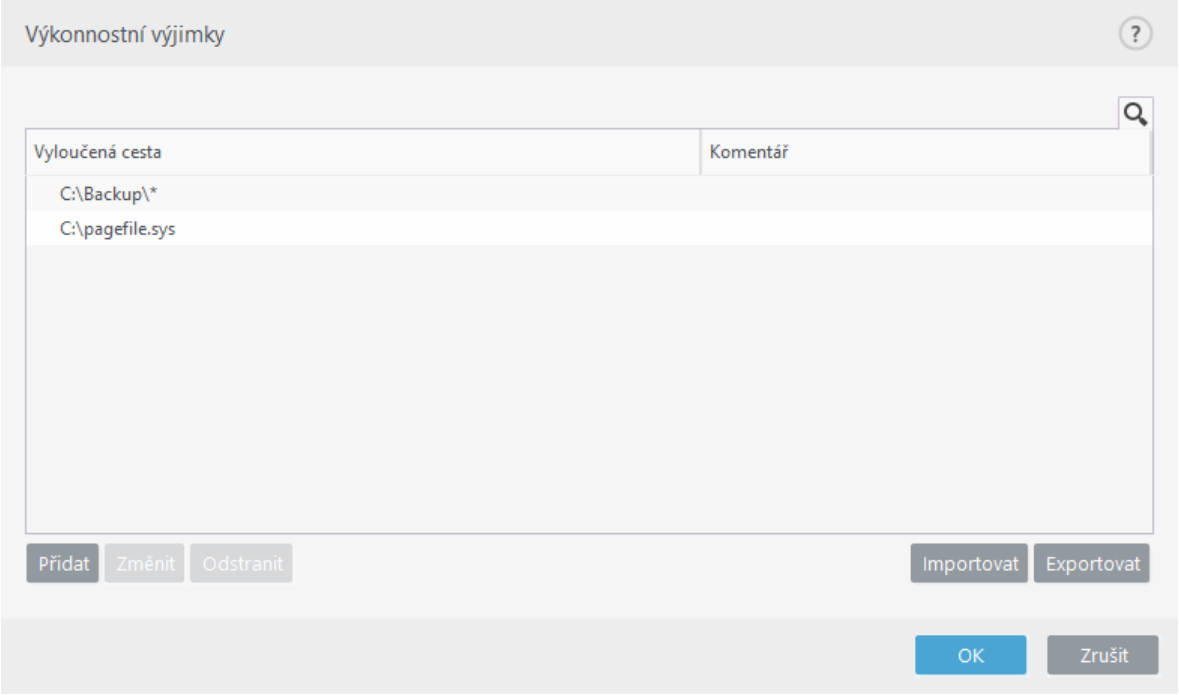
Výkonnostní výjimky

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** (dostupných po stisknutí klávesy F5 v hlavním okně programu) v sekci **Detekční jádro > Výjimky, kde klikněte na Změnit na řádku Výkonnostní výjimky**.

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":"9.1.2060","path":"Settings.ExclusionsManageme
nt.PerformanceExclusions","columns":["Path","Description"]}

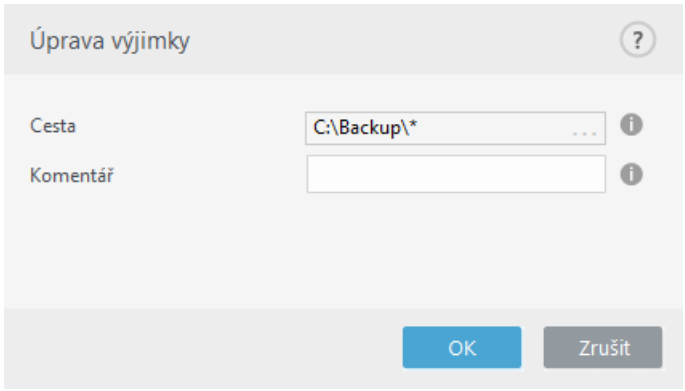
C:\Backup\*,custom comment

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:
• V této části nejsou dostupná tlačítka (nahoru/dolů) pro ovlivnění priority výjimek.
• 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

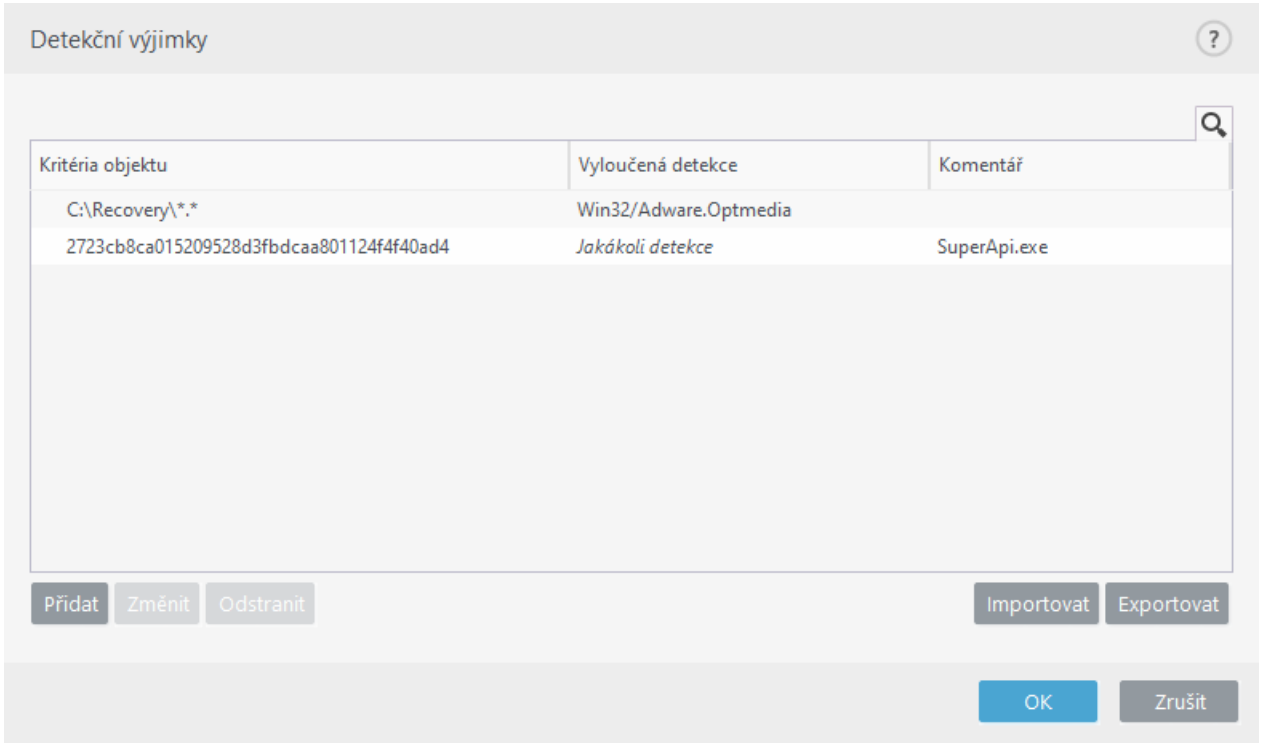
Při definování výjimky podle cesty můžete použít následující proměnné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

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** (dostupných po stisknutí klávesy F5 v hlavním okně programu) v sekci > **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":"9.1.2060","path":"Settings.ExclusionsManageme
nt.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileH
ash"]}

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

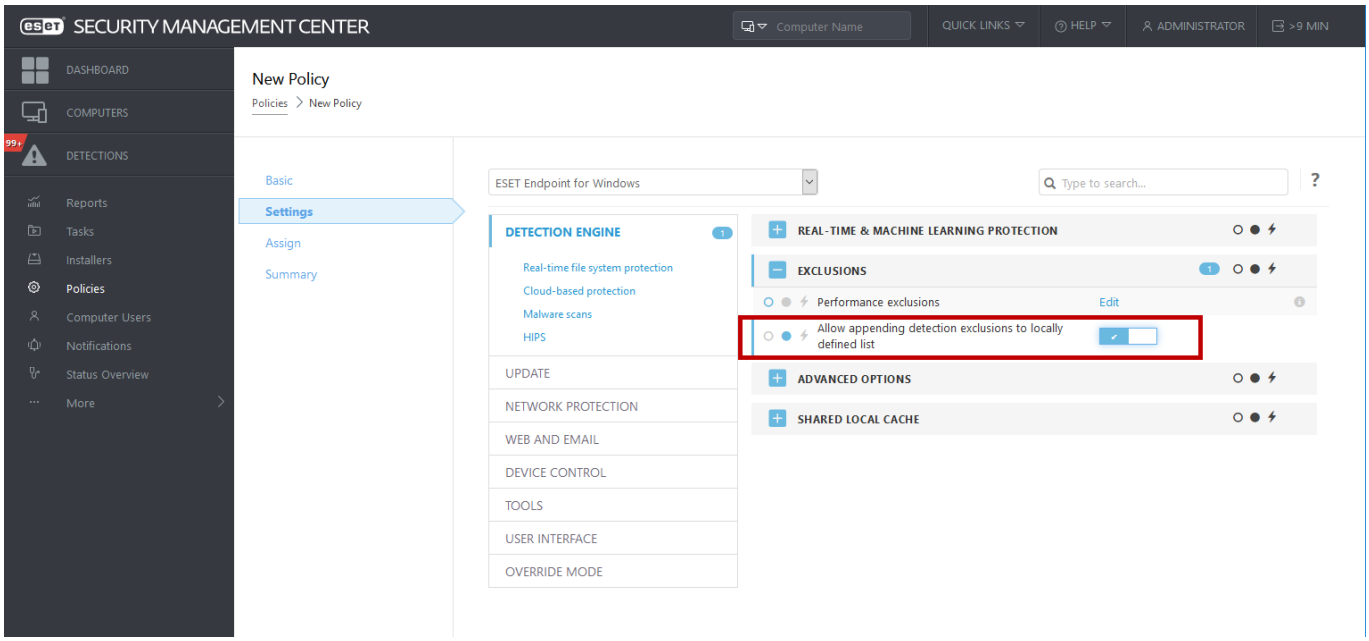
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Nastavení detekčních výjimek v ESET PROTECT

V ESET PROTECT je od verze 8.0 dostupný nový průvodce pro správu detekčních výjimek, prostřednictvím kterého můžete výjimky aplikovat na konkrétní počítače nebo skupiny.

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.

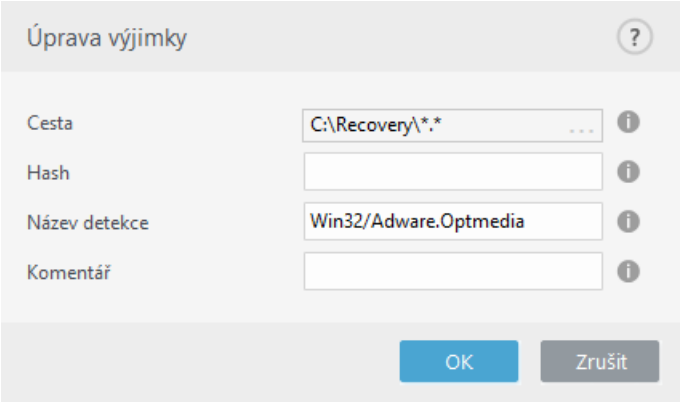


Přidání a úprava detekčních výjimek

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 Antivirus 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.

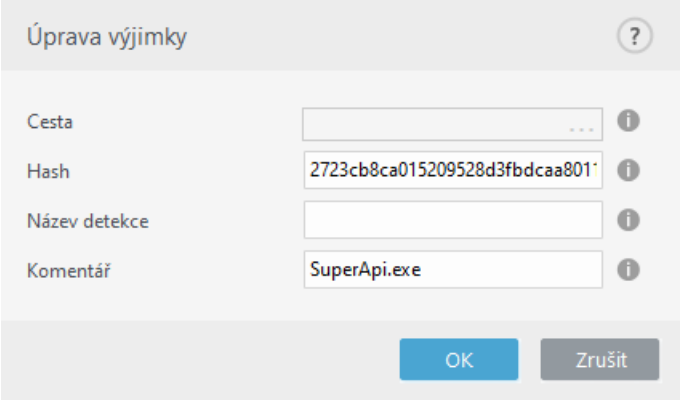
Další informace naleznete v kapitole Formát výjimky podle cesty.



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 Antivirus:
@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**.

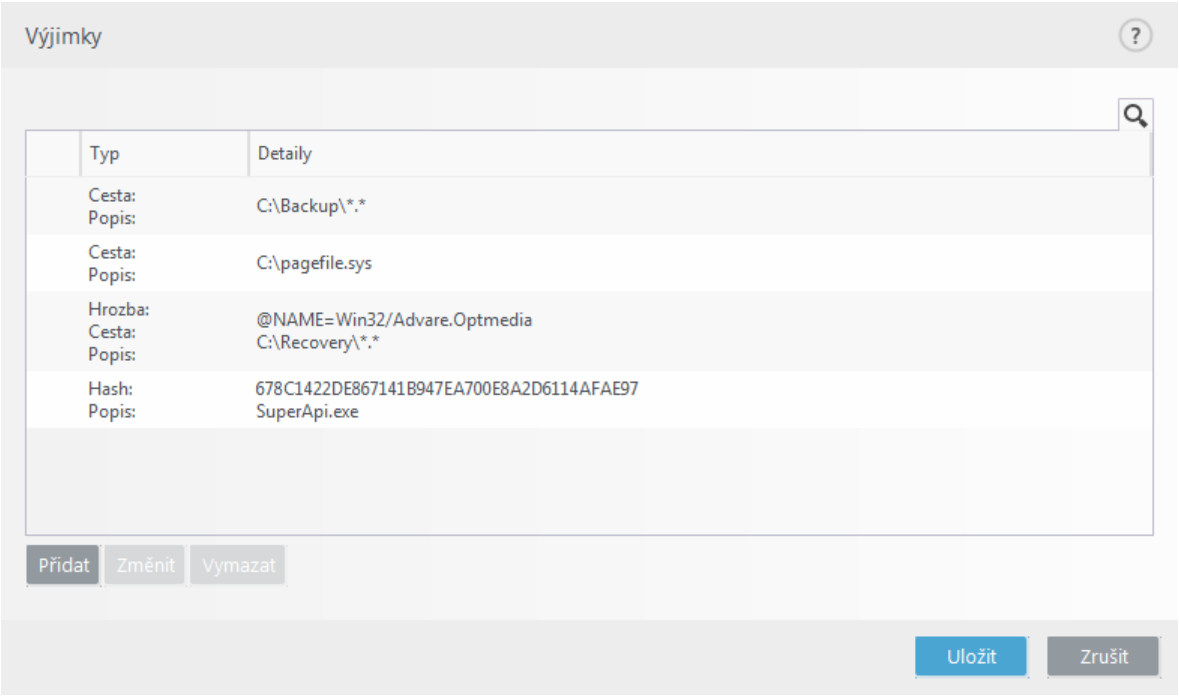
- **Konkrétní soubory** – pomocí této možnosti vyloučíte konkrétní soubor podle jeho SHA-1 kontrolního součtu.
- **Detekce** – pomocí této možnosti vyloučíte v každém souboru konkrétní detekci.
- **Cesta + Detekce** – pomocí této možnosti vyloučíte v konkrétním souboru (například *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*)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

Na základě typu detekce je vždy předvybrána doporučená možnost.

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

Výjimky (ve verzi 7.1 a starší)

Ve verzi 7.1 a starších byla konfigurace Výkonnostních výjimek a Detekčních výjimek společná.



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. Ke stejným problémům může dojít také při pokusu o živou migraci virtuálních strojů. 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.

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*).

Spustitelný soubor můžete na seznam výjimek přidat v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu v sekci **Detekční jádro > 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 Antivirus 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 Antivirus 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**.

HIPS výjimky

Prostřednictvím výjimek můžete vyloučit procesy z HIPS Hloubkové analýzy chování.

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**.

Pro více informací přejděte do kapitoly Výjimky.

Parametry skenovacího jádra 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.

V nastavení skenovacího jádra ThreatSense můžete definovat následující parametry:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

Pro zobrazení nastavení klikněte na záložku **Parametry skenovacího jádra ThreatSense** v Rozšířeném nastavení jakéhokoli modulu, který používá ThreatSense technologii (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 Antivirus 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 chcete zkontrolovat.

Ostatní

Při konfiguraci parametrů skenovacího jádra ThreatSense jsou v sekci **Ostatní** k dispozici 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

Možnosti pro definování úrovně léčení naleznete v konfiguraci jednotlivých modulů (například **Rezidentní ochrany souborového systému**) v části **Parametry skenovacího jádra ThreatSense** > **Léčení**.

V případě rezidentní ochrana i dalších modulech jsou k dispozici níže uvedené úrovně léčení.

Řešení infekce v ESET Endpoint Antivirus 9

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.
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

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení parametrů skenovací jádra ThreatSense můžete definovat typy souborů, které chcete zkontrolovat.

Nezaměňujte mezi sebou jednotlivé typy výjimek:

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`).

Pro zobrazení přípony konkrétního souboru si zobrazte detailní informace o souboru (z kontextového menu vyberte možnost Vlastnosti) nebo si deaktivujte možnost **Skrýt přípony souborů známých typů** přímo v Průzkumníku Windows (**Ovládací panely** > **Možnosti složky** > **Zobrazení**).

Doplňující parametry skenovacího jádra ThreatSense

Doplňující parametry ThreatSense pro nově vytvořené a změněné soubory – pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s přidanými parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána pokročilá heuristika, 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 archivy (interně komprimované spustitelné soubory). Standardně jsou archivy kontrolovány do 10 úrovní vnoření bez ohledu na jejich velikost. Pro změnu kontroly archivů odškrtněte možnost **Standardní nastavení archivů.**

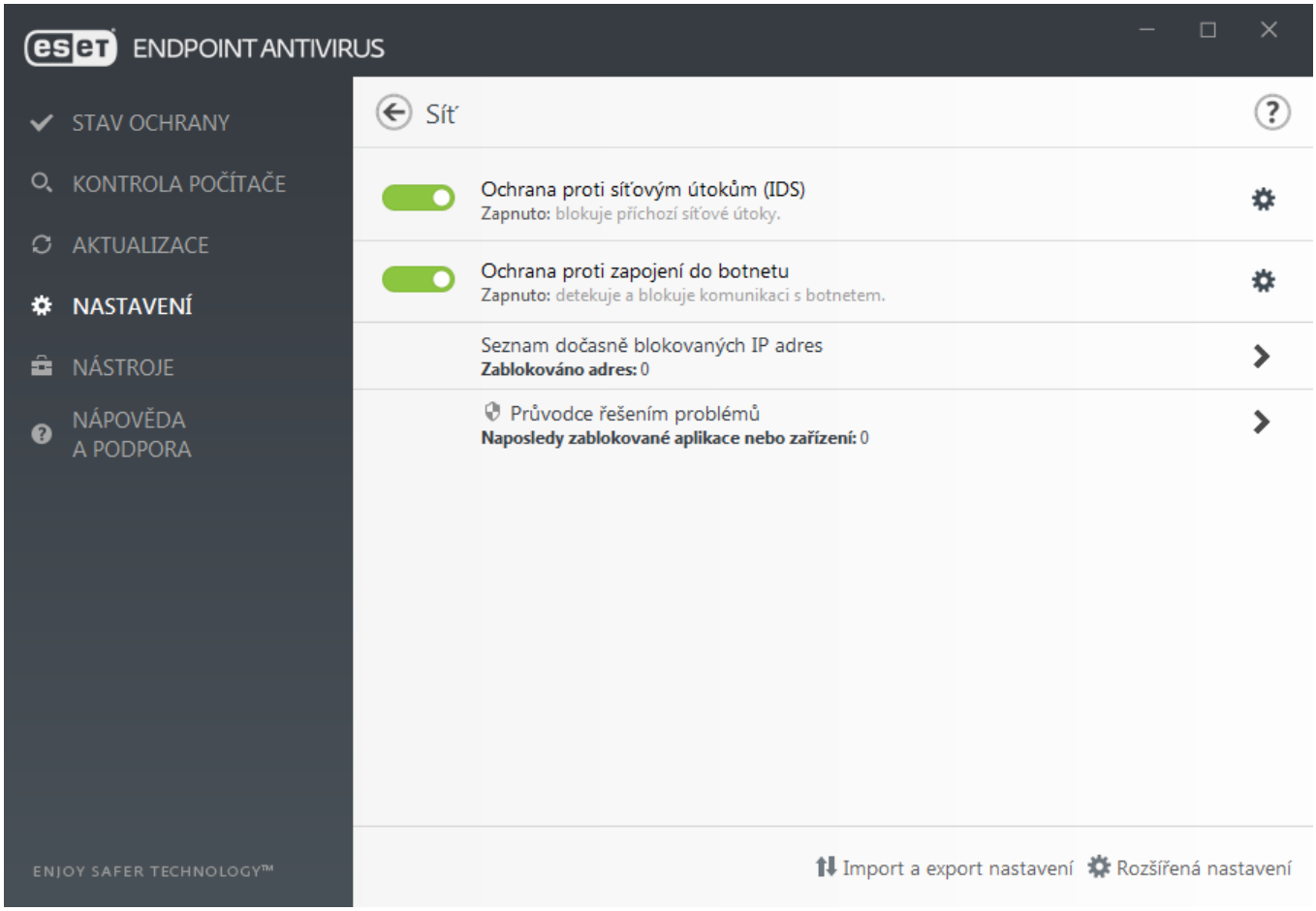
Více informací o Runtime archivech, Samorozbalovacích archivech a Rozšířené heuristice naleznete v kapitole Parametry skenovacího jádra ThreatSense.

Doplňující parametry ThreatSense pro spouštěné soubory – standardně se Rozšířená heuristika se používá pro spouštěné soubory. Pokud je zapnutá, důrazně doporučujeme ponechat zapnutou také Smart optimalizaci a ESET LiveGrid® pro snížení dopadu na výkon systému.

Síť

V sekci **Síť** máte rychlý přístup k následujícím komponentám, případně jejich konfiguraci v **Rozšířeném nastavení**:

- **Ochrana proti síťovým útokům (IDS)** – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Komunikace vyhodnocená jako škodlivá, bude blokována. Zároveň vás ESET Endpoint Antivirus upozorní na případy, kdy se připojujete k nezabezpečené nebo slabě zabezpečené bezdrátové síti.
- **Ochrana proti zapojení do botnetu** – tato funkce zajišťuje ochranu před škodlivým kódem, který se počítač snaží zapojit do botnetu. Ochranu proti zapojení do botnetu můžete dočasně deaktivovat pomocí přepínače  (nedoporučujeme).
- **Seznam dočasně blokovaných IP adres** – zobrazí seznam IP adres, ze kterých byl zjištěn útok na tento počítač, a z tohoto důvodu byla dočasně zablokována komunikace z těchto adres. Pro více informací klikněte na tuto možnost a následně stiskněte klávesu F1.
- **Průvodce řešením problémů** – pomáhá s řešením problémů se síťovou komunikací, kterou ovlivnil ESET firewall. Pro více informací přejděte do kapitoly Průvodce řešením problémů.



Ochrana proti síťovým útokům

Ochrana 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 – pomocí této možnosti můžete detailně přizpůsobit možnosti detekce mnoha typů útoků a zranitelností, které mohou poškodit váš počítač.

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. Pro konfiguraci Ochrana proti útokům hrubou silou přejděte v hlavním okně programu na záložku **Nastavení**, klikněte na tlačítko **Rozšířená nastavení** (F5) a dále do sekce **Síťová ochrana** > **Ochrana proti síťovým útokům** > **Ochrana proti útokům hrubou silou**.

Zapnout ochranu proti útoku hrubou silou – tato součást produktu ESET Endpoint Antivirus 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

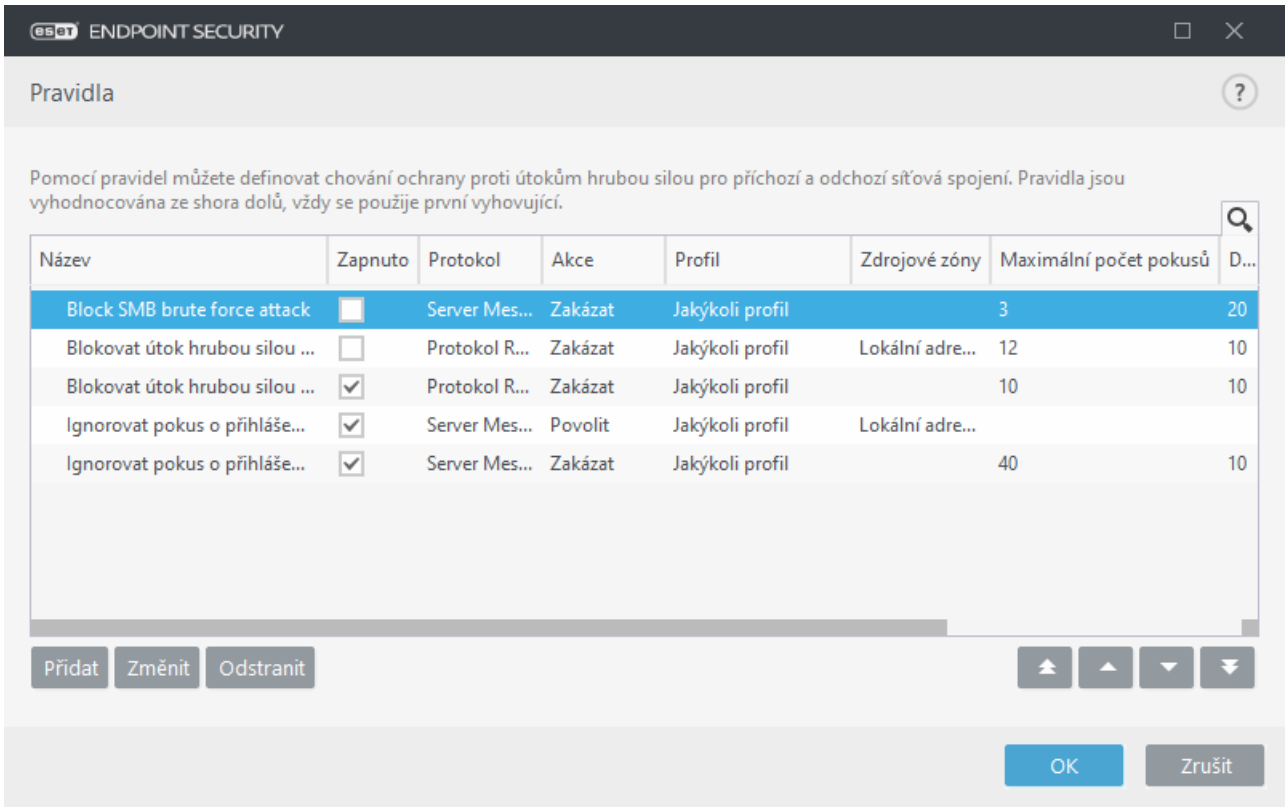
a odchozí síťová spojení, stejně tak si vytvářet vlastní a kdykoli je upravovat. Pro více informací přejděte do kapitoly Pravidla.

Výjimky – seznam detekcí vyloučených z kontroly definovaný na základě IP adresy nebo cesty k aplikaci. Výjimky je možné vytvářet a upravovat prostřednictvím vaší ESET PROTECT konzole. Pro více informací přejděte do kapitoly 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.

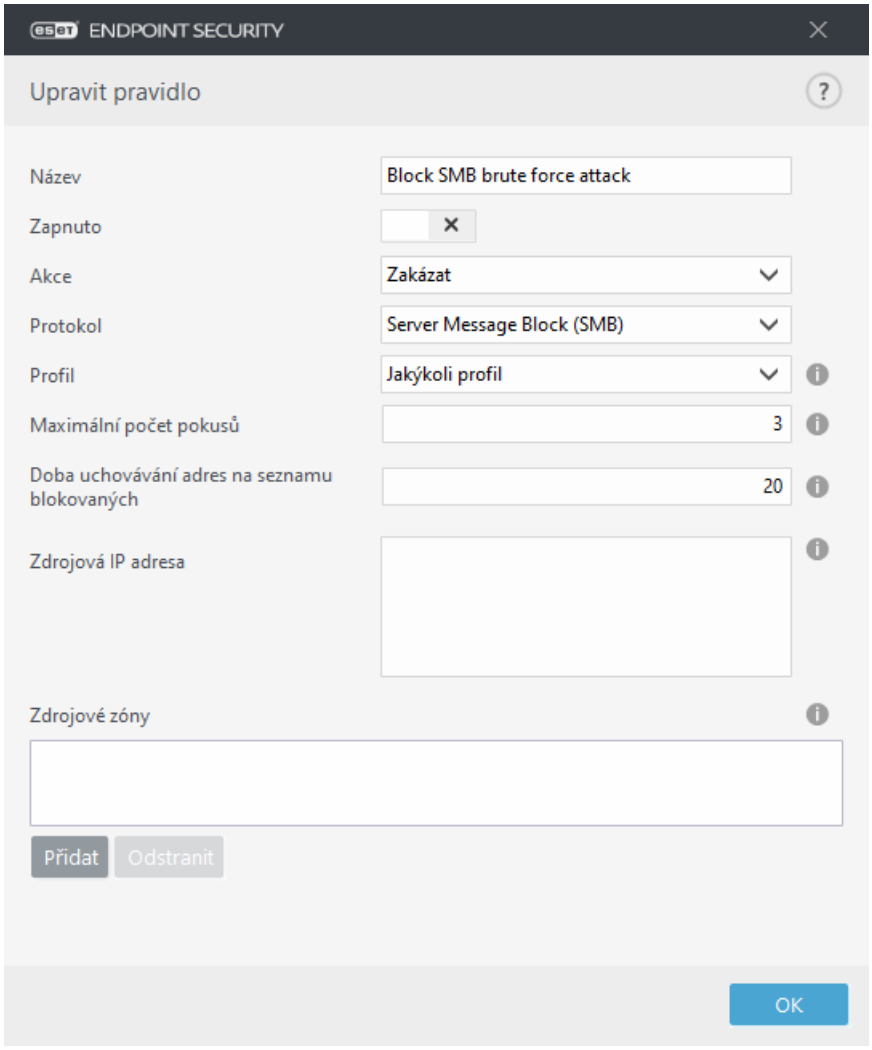
Správa pravidel ochrany proti útokům hrubou silou



- **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.
- **Šipky Nahoru/Výše/Dolů/Níže** – pomocí těchto tlačítek změníte pořadí vyhodnocování pravidel (vyhodnocována 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 – odškrtněte tuto možnost, pokud chcete ponechat pravidlo v seznamu pravidel a 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 – pro jednotlivé profily můžete definovat vlastní pravidla.

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 adres oddělte čárkou.

Zdrojové zóny – po kliknutí na tlačítko **Přidat** si můžete vybrat z předdefinovaných zón nebo si vytvořit vlastní na základě rozsahu IP adresu.

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.

Rozšířené možnosti filtrování

V sekci Ochrana proti síťovým útokům můžete konfigurovat rozšířené možnosti filtrování síťové komunikace za účelem detekce různých typů útoků a zranitelností, které by mohly ohrozit váš počítač.

V některých případech neobdržíte oznámení o hrozbě týkající se blokované komunikace. Informace o tom, jak zobrazit veškerou zablokovanou komunikaci, naleznete v kapitole Protokolování a vytváření pravidel nebo výjimek z protokolu.

Dostupnost jednotlivých možností v **Rozšířeném nastavení** (F5) > **Síťová ochrana** > **Ochrana proti síťovým útokům** může záviset na typu nebo verzi bezpečnostního produktu ESET a modulu firewallu, stejně tak vašem operačním systému. Některé funkce jsou dostupné pouze v ESET Endpoint Security.

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).
- **Blokovat nebezpečnou adresu po detekci útoku** – pokud je zjištěn útok z určité adresy, veškerá komunikace z ní bude blokována.

- **Zobrazit upozornění po detekci útoku** – po detekci útoku se zobrazí upozornění v pravém dolním rohu obrazovky.
- **Zobrazit upozornění při pokusu o zneužití bezpečnostních děr** – 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.
- **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).

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 Antivirus
- Vytvoření IDS pravidla pro klientskou stanici prostřednictvím ESET PROTECT

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.
- **Blokovat** – nad každým systémovým procesem bude provedena standardní akce (povolit nebo blokovat). Pro změnu výchozího chování produktu ESET Endpoint Antivirus 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 Antivirus. Možnost **Ne** vyberte, pokud nechcete událost zaznamenat do protokolu. Dostupné možnosti: **Výchozí akce**/**Ano**/**Ne**.

Záložka Výjimky bude dostupná v případě, kdy administrátor vytvoří IDS výjimku v ESET PROTECT Web Console. Na seznamu IDS výjimek se mohou nacházet pouze povolovací pravidla. Vyhodnocována jsou dříve, než IDS pravidla.

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 (vyhodnocována jsou ze shora dolů).

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 Antivirus.
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 požadované upozornění, například **SMB relace bez bezpečnostního rozšíření**.
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**.

Zablokována podezřelá hrozba

Tato událost může nastat v případě, kdy se některá aplikace na vašem počítači pokouší nestandardně komunikovat s jiným počítačem v síti, zneužít bezpečnostní díru nebo skenovat porty.

Hrozba – název hrozby.

Zdroj – zdrojovou síťovou adresu,

Cíl – cílovou síťovou adresu,

Zastavit blokování – kliknutím vytvoříte IDS pravidlo pro danou podezřelou hrozbu takové, že bude komunikace povolena.

Nadále blokovat – kliknutím zablokujete detekovanou hrozbu. Pro vytvoření IDS pravidla pro tuto hrozbu zaškrtněte možnost **Znovu neupozorňovat**.

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.

Řešení problémů v síťové ochraně

Tento průvodce vám pomůže při řešení síťových problémů způsobených ESET firewallem. 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 stále komunikace nebude fungovat nebo problémy s aplikací/zařízením přetrvávají, vyberte možnost **Aplikace stále nefunguje** a veškerá komunikace aplikace/zařízení bude povolena. V případě přetrvávajících problémů doporučujeme před pokračováním restartovat počítač. Některá pravidla se uplatní až při dalším startu systému.

Pro zobrazení pravidel, které vytvořil průvodce, klikněte na možnost **Zobrazit změny**.

Pokud potřebujete odblokovat komunikaci další aplikace nebo zařízení klikněte na možnost **Odblokovat další**.

Známé sítě

Pokud počítač často připojujete k veřejným sítím nebo sítím mimo vaši pracovní síť, doporučujeme vám ověřit důvěryhodnost takových sítí. Po prvotním definování sítě, ESET Endpoint Antivirus může rozpoznat důvěryhodnou síť na základě parametrů definovaných v sekci **Identifikace sítě**. To je užitečné pro počítače, které se připojují často do sítí s IP adresami podobnými důvěryhodné zóně. V některých případech, ESET Endpoint Antivirus může prohlásit neznámou síť za důvěryhodnou. Pro eliminaci takového případu doporučujeme používat možnost **Autentifikace sítě**.

Po připojení počítače k síti nebo změně konfigurace sítě prohledá ESET Endpoint Antivirus seznam známých sítí, zda pro ni nenalezne odpovídající záznam. V případě, že **Identifikace sítě** a **Autentifikace sítě** (nepovinné) bude vyhovovat záznamu, síť bude označená jako připojená. V případě, že nebude nalezena žádná známá síť, vytvoří se nová na základě zjištěné konfigurace sítě. Standardně se pro ni použije přísný režim ochrany (bude označena **Veřejná síť**). Po připojení k takové síti se zároveň zobrazí dialog **Zjištěno připojení** k nové síti, pomocí kterého můžete nastavit režim ochrany v síti – **Důvěryhodná síť**, **Nedůvěryhodná síť**, případně můžete vybrat možnost **Převzít nastavení z Windows**. Pokud se připojíte k již známé síti, jejíž režim ochrany je nastaven na **Důvěryhodná síť**, všechny podsítě této sítě budou přidány do důvěryhodné zóny.

Typ ochrany nové sítě – vyberte některou z následujících možností, která se použije automaticky při připojení do nové sítě: Převzít nastavení z Windows, Dotázat se uživatele nebo Označit síť jako veřejnou.

> Pokud vyberete možnost **Převzít nastavení z Windows**, dialogové okno pro výběr typu sítě se nezobrazí a automaticky se převezme nastavení z centra sítí a sdílení ve Windows. V případě nesprávného nastavení sítě ve Windows to může znamenat, že budou běžné síťové funkce (například sdílení souborů nebo vzdálená plocha) dostupné na veřejných sítích, což představuje bezpečnostní riziko.

Známé sítě můžete konfigurovat ručně pomocí Editoru známých sítí.

Editor známých sítí

Seznam známých sítí můžete konfigurovat ručně v **Rozšířeném nastavením** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **Síťová ochrana** > **Obecné** > **Známé sítě** po kliknutí na **Změnit** na řádku **Známé sítě**.

Sloupce

Název – název známé sítě.

Typ ochrany – zobrazuje jednu z těchto možností: **Důvěryhodná firemní síť**, **Nedůvěryhodná síť** nebo **Převzít nastavení z Windows**.

Profil firewallu – zobrazuje profil, jaký bude uplatňován na komunikaci v dané síti. Standardně se nabízí **Převzít ze síťového adaptéru**.

Aktualizační profil – zobrazuje aktualizační profil, který se použije při připojení k dané síti.

Ovládací prvky

Přidat – kliknutím přidáte novou známou síť.

Změnit – kliknutím upravíte existující známou síť.

Odstranit – vyberte síť, kterou chcete **odstranit** a klikněte na toto tlačítko.

 **Nahoru/Výše/Dolů/Níže** – pomocí těchto tlačítko změníte pořadí vyhodnocování známých sítí (vyhodnocovány jsou ze shora dolů).

Nastavení sítě je rozloženo do následujících záložek.

Síť

V této sekci můžete definovat **název sítě** a **typ její ochrany** (Důvěryhodná síť, Nedůvěryhodná síť nebo Převzít nastavení z Windows). Pomocí rozbalovacího menu **Profil firewallu** vyberte požadovaný profil pro tuto síť. Pokud nastavíte režim ochrany na **Důvěryhodná síť**, všechny připojené podsítě budou 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, všechny budou považovány za důvěryhodné, bez ohledu na nastavení **Identifikace sítě**.

Další adresy zadané do pole **Další důvěryhodné adresy** budou vždy přidány do důvěryhodné zóny adaptéru připojeného do této sítě (bez ohledu na režim ochrany sítě).

Upozornit na slabě zabezpečenou Wi-Fi síť – po aktivování této možnosti vás ESET Endpoint Antivirus upozorní při připojení nezabezpečené nebo slabě zabezpečené bezdrátové síti.

Profil firewallu – vyberte profil, který se použije pro ochranu při připojení k této síti.

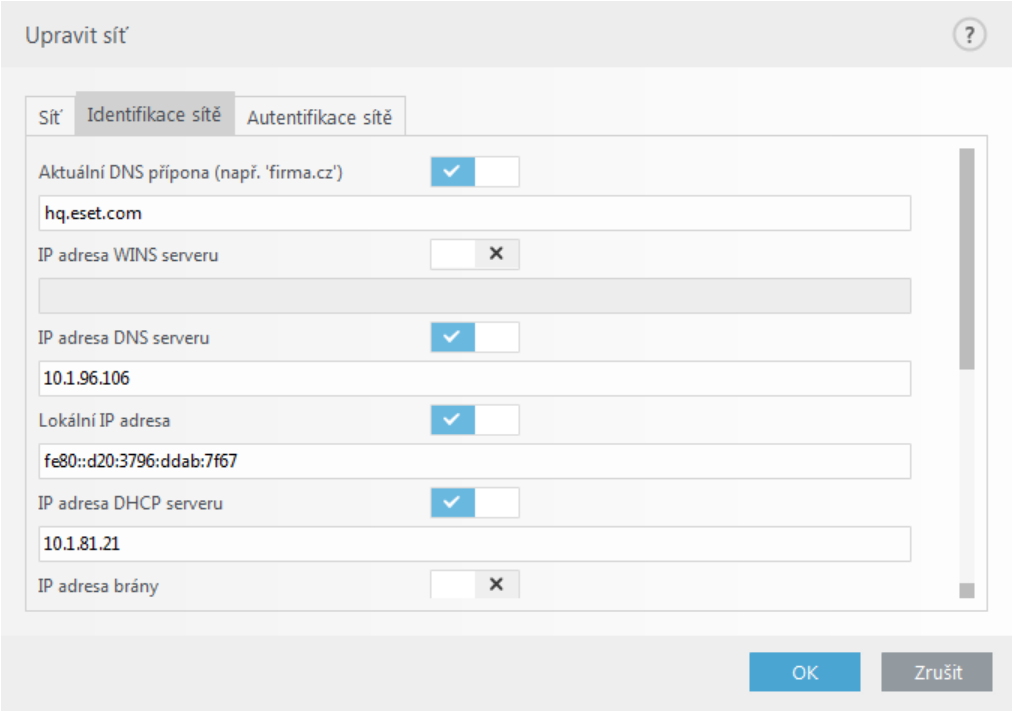
Aktualizační profil – vyberte profil, který se použije pro aktualizaci při připojení k této síti.

Následující parametry je nutné splnit, aby mohla být označená jako připojená v seznamu připojených sítí:

- **Identifikace sítě** – všechny vyplněné parametry musí odpovídat parametrům aktivního připojení.
- **Autentifikace sítě** – pokud je vybrán autentifikační server, musí dojít k úspěšnému ověření vůči ESET Authentication Serveru.

Identifikace sítě

Identifikace sítě probíhá na základě parametrů adaptéru lokální sítě. Identifikace je úspěšná, pokud definované parametry odpovídají aktivnímu připojení do sítě. Podporovány jsou IPv4 i IPv6 adresy.



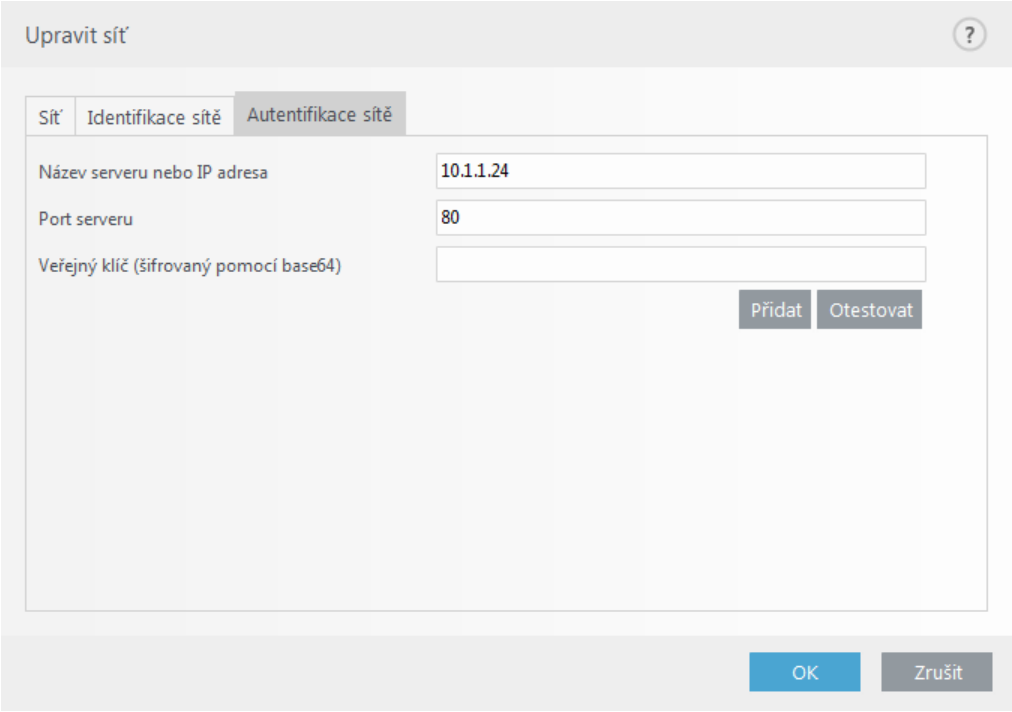
Autentifikace sítě

Autentifikace zóny vyhledává v síti specifický server a pro vlastní autentifikaci vůči serveru používá asymetrické šifrování (RSA). Název autentifikované sítě musí odpovídat názvu sítě definovaném v nastavení autentifikačního serveru. Zadejte název serveru, port, na kterém poslouchá server a veřejný klíč, který odpovídá soukromému klíči serveru (více naleznete v kapitole Autentifikace sítě – konfigurace serveru). Název serveru je zadejte jako IP adresu, DNS nebo NetBios jméno. Za názvem serveru může následovat cesta upřesňující umístění klíče na serveru (např. jméno_serveru/složka1/složka2/autentifikace). Také můžete zadat více serverů, oddělených středníkem.

Stáhnout ESET Authentication Server

Zdroj, ze kterého se bude načítán veřejný klíč, může být soubor typu:

- PEM kryptovaný veřejný klíč (.pem). Tento klíč je možné vygenerovat prostřednictvím ESET Authentication Serveru (další informace naleznete v kapitole Autentifikace sítě – konfigurace serveru).
- Šifrovaný veřejný klíč
- Certifikát s veřejným klíčem (.crt)



Pro ověření nastavení klikněte na tlačítko **Otestovat**. V případě úspěšné autentizace se zobrazí oznámení Autentifikace proběhla úspěšně. Pokud není konfigurace správně nastavena, zobrazí se některé z následujících chybových hlášení:

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.

Autentifikace zóny – nastavení serverové části

Autentifikace může být spuštěna na libovolném počítači/serveru připojeném do sítě, která má být autentifikována. Aplikace ESET Authentication Server musí být na počítači/serveru nainstalována a běžet, aby bylo možné provést autentifikaci kdykoliv při pokusu o připojení klienta do sítě. Instalační soubor aplikace ESET Authentication Server je možné stáhnout z webových stránek společnosti ESET.

Po nainstalování ESET Authentication Server se zobrazí hlavní okno autentifikačního serveru, které je možné později kdykoli vyvolat ručně z nabídky **Start** > **Programy** > **ESET** > **ESET Authentication Server**.

Konfigurace autentifikačního serveru spočívá v zadání názvu autentifikační síte, definování portu, na kterém bude server naslouchat (standardně 80) a místě uložení páru privátního a veřejného klíče. Dále vygenerujte veřejný a privátní klíč, který bude použit v procesu ověřování. Soukromý klíč zůstává na autentifikačním serveru, veřejný klíč je potřeba vložit na klientské straně do nastavení zón firewallu.

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 Antivirus 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.

Jak nastavit zóny

Zóna představuje skupinu síťových adres, které dohromady tvoří logickou skupinu IP adres. To je užitečné při opakovaném použití stejné sady adres ve více pravidlech. Každá adresa ve skupině má daná práva, která jsou platná pro celou skupinu. Příkladem takové skupiny je **Důvěryhodná zóna**. Důvěryhodná zóna představuje skupinu síťových adres, které nejsou firewallem nijak blokovány. Zóny můžete spravovat v **rozšířeném nastavení** v sekci **Síťová ochrana** > **Obecné** > **Zóny**, kde klikněte na **Změnit** na řádku **Zóny**. Pro vytvoření nové zóny klikněte v zobrazeném dialogovém okně na tlačítko **Přidat**, zadejte její **Název**, **Popis** a přidejte vzdálenou IP adresu do pole **Vzdálená adresa počítače (IPv4/IPv6, rozsah, maska)**. Další informace naleznete v kapitole Zóny firewallu.

Zóny firewallu

Pro více informací o zónách přejděte do kapitoly Nastavení zón.

Sloupce

Název – název skupiny vzdálených počítačů.

IP adresa – vzdálená adresa identifikují zónu.

Ovládací prvky

Pro manipulaci s jednotlivými záznamy použijte tlačítka **přidat**, **změnit** nebo **odebrat**.

Název – název skupiny vzdálených počítačů.

Popis – obecný popis skupiny.

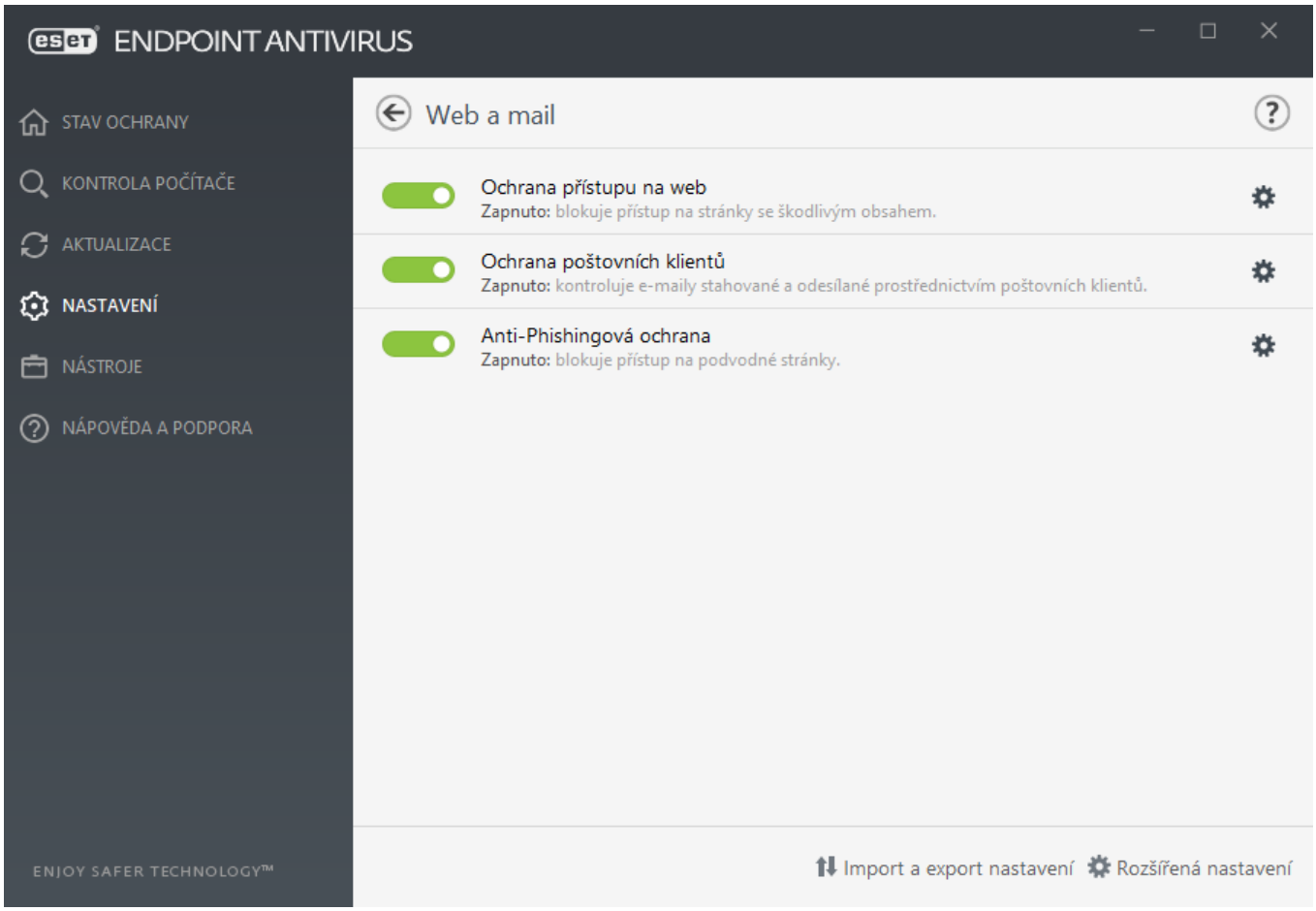
Vzdálená adresa počítače (IPv4, IPv6, rozsah, podsíť) – umožní přidat vzdálenou adresu, rozsah adres nebo podsíť.

Odstranit – odebere zónu ze seznamu.

Mějte na paměti, že předdefinované zóny není možné odstranit.

Web a mail

Konfiguraci webu a e-mailu naleznete na záložce **Nastavení**, po kliknutí na část **Web a mail**. Odtud se také dostanete k detailnímu nastavení programu.



Internetové připojení se stalo u počítačů standardem. Bohužel se stalo i hlavním médiem pro šíření škodlivého kódu. Proto je velmi důležité věnovat zvýšenou pozornost nastavení v části **Ochrana přístupu na web**.

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 Antivirus kontrolu veškeré komunikace.

Anti-Phishingová ochrana blokuje přístup na podvodné stránky vytvořené za účelem cílem získat od uživatele hesla a další citlivé informace. Konfiguraci Anti-Phishingové ochrany naleznete v hlavním okně programu na záložce Nastavení > Web a mail. Pro více informací přejděte do kapitoly Anti-Phishingová ochrana.

Také můžete moduly webové/e-mailové/anti-phishingové ochrany dočasně vypnout pomocí přepínače .

Filtrování protokolů

Antivirovou ochranu aplikačních protokolů zajišťuje skenovací jádro ThreatSense, které obsahuje všechny pokročilé metody detekce škodlivého kódu. Filtrování protokolů pracuje zcela nezávisle na použitém internetovém prohlížeči, nebo poštovním klientovi. Pro úpravu nastavení kontroly šifrované komunikace (SSL) přejděte do **Rozšířeného nastavení** (F5) > **Web a mail** > **SSL/TLS**.

Pro kontrolu šifrované komunikace (SSL) přejděte do sekce Web a mail > Kontrola protokolu SSL/TLS. pokud tuto možnost vypnete, některé moduly ESET Endpoint Antivirus, které závisí na této funkci (například Ochrana přístupu na web, Ochrana poštovních klientů, Anti-Phishing, Filtrování obsahu webu), nebudou fungovat.

Vyloučené aplikace – pomocí této možnosti můžete vyloučit konkrétní aplikaci z filtrování protokolů. To může být užitečné při řešení problémů

Vyloučené IP adresy – pomocí této možnosti můžete vyloučit konkrétní adresu z filtrování protokolů. To může být užitečné při řešení problémů

Adresa IPv4 a masky:
• *192.168.0.10* – IP adresa samostatného počítače, pro který má pravidlo platit.
• *192.168.0.1* až *192.168.0.99* – Počáteční a konečná adresa IP adresa k určení rozsahu IP (u několika počítačů), pro které se má pravidlo použít.
• Podsíť (skupina počítačů) definovaná pomocí adresy IP a masky. Příklad: *255.255.255.0* je maska podsítě pro prefix *192.168.1.0/24*, což znamená rozsah adres od *192.168.1.1* do 192.168.1.254.
Adresa IPv6 a masky:
• *2001:718:1c01:16:214:22ff:fec9:ca5* – IPv6 adresa samostatného počítače, pro který má pravidlo platit.
• *2002:c0a8:6301:1::1/64* – Adresa IPv6 s prefixem o délce 64 bitů, to znamená od *2002:c0a8:6301:0001:0000:0000:0000:0000 do 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff.*

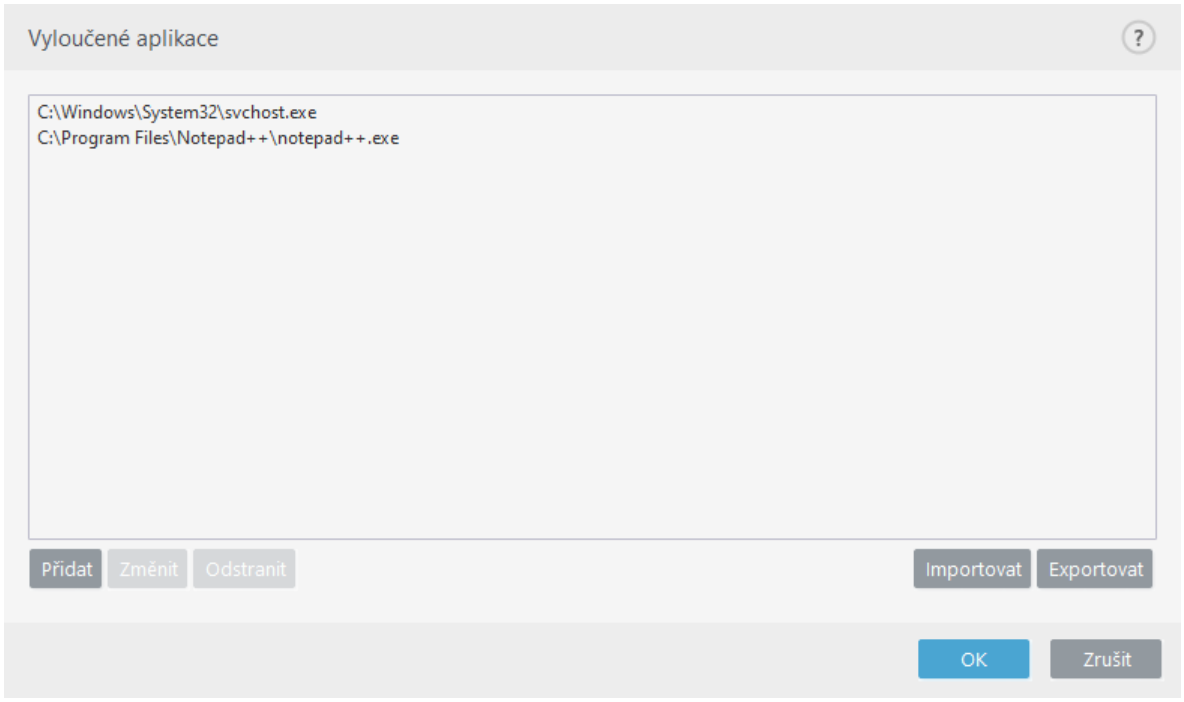
Vyloučené aplikace

Pokud potřebujete vyloučit síťovou komunikaci aplikace z modulu filtrování protokolů, přidejte ji na tento seznam. Následně nebude HTTP, POP3 a IMAP komunikace vybraných aplikací kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze ve výjimečných případech, například pokud aplikace v důsledku kontroly komunikace nepracuje správně.

Spuštěné aplikace a běžící služby se zobrazí automaticky. Pomocí tlačítka **Přidat** ručně vyberte cestu k aplikaci, kterou chcete přidat do seznamu výjimek z filtrování protokolů.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Vyloučené IP adresy

Obsah nacházející se na IP adresách uvedených na tomto seznamu bude modul filtrování protokolů ignorovat To znamená, že komunikace prostřednictvím protokolů HTTP, POP3 a IMAP na/z těchto 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.



SSL/TLS

ESET Endpoint Antivirus dokáže detekovat hrozby rovněž v komunikaci zapouzdřené v protokolu SSL. Kontrolu můžete přizpůsobit podle toho, zda je certifikát využíván danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola komunikace chráněná SSL protokolem SSL.

Zapnout filtrování protokolu SSL/TLS – filtrování protokolů je standardně zapnuté. Vypnout filtrování protokolu SSL/TLS můžete v **Rozšířeném nastavení** v sekci **Web a mail** > **SSL/TLS** nebo prostřednictvím politiky. Pokud filtrování vypnete, program nebude kontrolovat šifrovanou SSL komunikaci.

K dispozici jsou následující **režimy filtrování SSL/TLS protokolu**:

Režim filtrování	Popis
Automatický režim	Výchozí režim, ve kterém je kontrolována pouze komunikace vybraných aplikací, jako jsou webové prohlížeče a poštovní klienti. V případě potřeby můžete kdykoli rozšířit seznam aplikací, jejichž komunikaci chcete kontrolovat.
Interaktivní režim	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 využívající nedůvěryhodný certifikát označený jako důvěryhodný (v seznamu důvěryhodných certifikátů) bude komunikace povolena a přenášený obsah bude filtrován.

Pomocí **seznamu SSL/TLS filtrovaných aplikací** můžete přizpůsobit chování ESET Endpoint Antivirus pro konkrétní aplikace využívající šifrovaný kanál.

Pomocí **seznamu známých certifikátů** můžete přizpůsobit chování ESET Endpoint Antivirus při detekci konkrétních SSL certifikátů.

Nekontrolovat komunikaci s důvěryhodnými doménami – pokud je tato možnost aktivní, komunikace s doménami uvedenými na interním seznamu důvěryhodných domén nebude kontrolována. Důvěryhodnost domény je určena vestavěným whitelistem.

Blokovat šifrovanou komunikaci používající zastaralý protokol SSL v2 – komunikace využívající starší verzi protokolu SSL bude automaticky blokována.

> Pokud máte aktivní možnost **Nekontrolovat komunikaci s důvěryhodnými doménami**, kontrola komunikace s těmito doménami bude automaticky vyloučena.

Kořenový certifikát

Kořenový certifikát – pro správné fungování kontroly SSL komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost **Přidat kořenový certifikát do známých prohlížečů** by měla být zapnuta. Výběrem této možnosti zajistíte automatické přidání kořenového certifikátu společnosti ESET do známých prohlížečů

(například prohlížeče Opera nebo Firefox). Do prohlížečů využívajících systémové úložiště kořenových certifikátů se certifikát přidá automaticky (například prohlížeče Internet Explorer).

V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát** > **Detaily** > **Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

Platnost certifikátu

Pokud nelze ověřit důvěryhodnost certifikátu – v některých případech nelze certifikát webové stránky ověřit pomocí systémového úložiště kořenových certifikátů (TRCA). To znamená, že certifikát je někým samostatně podepsán (například administrátorem webového serveru nebo malou firmou) a považování tohoto certifikátu za důvěryhodný nemusí vždy představovat riziko. Většina velkých obchodních společností (například banky) používají certifikát podepsaný certifikační autoritou (Trusted Root Certification Authorities). Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** vždy zablokujete komunikaci s webovou stránkou využívající nedůvěryhodný certifikát.

Pokud je certifikát poškozený – znamená to, že certifikát nebyl správně podepsán nebo je poškozený. V tomto případě doporučujeme **Zablokovat komunikaci využívající daný certifikát**. Pokud vyberete **Dotázat se uživatele na platnost certifikátů**, uživatel bude vyzván k výběru akce, kterou je třeba provést 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"

Certifikáty

Pro správné fungování kontroly SSL komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost **Přidat kořenový certifikát do známých prohlížečů** by měla být zapnuta. Výběrem této možnosti zajistíte automatické přidání kořenového certifikátu společnosti ESET do známých prohlížečů (například prohlížeče Opera nebo Firefox). Do prohlížečů využívajících systémové úložiště kořenových certifikátů se certifikát přidá automaticky (například prohlížeče Internet Explorer). V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát** > **Detaily** > **Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

V některých případech nelze certifikát webové stránky ověřit pomocí systémového úložiště kořenových certifikátů (TRCA). To znamená, že certifikát je někým samostatně podepsán (například administrátorem webového serveru nebo malou firmou) a považování tohoto certifikátu za důvěryhodný nemusí vždy představovat riziko. Většina velkých obchodních společností (například banky) používají certifikát podepsaný certifikační autoritou (TRCA). Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. V zobrazeném dialogovém okně pro výběr akce můžete rozhodnout, zda označit certifikát 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.

Pokud je certifikát neplatný nebo poškozený, znamená to, že certifikátu vypršela platnost nebo nebyl správně

podepsán. V tomto případě doporučujeme **zakázat komunikaci využívající daný certifikát**.

Šifrovaná síťová komunikace

Pokud je aktivní kontrola protokolu SSL/TLS, výstražné okno se seznamem dostupných akcí se zobrazí, pokud:

Webová stránka používá neověřený nebo neplatný certifikát a ESET Endpoint Antivirus 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.

Režim filtrování protokolu SSL/TLS nastaven na **Interaktivní**, pro každou webovou stránku se zobrazí dialogové okno s možností **Kontrolovat** nebo **Ignorovat** komunikaci. Některé aplikace ověřují, zda nedošlo ke změně SSL komunikace, případě inspekci přenášeného obsahu. V takovém případě je nutné pro zajištění funkčnosti aplikace vybrat možnost **Ignorovat**.

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"

V obou případech je dostupná možnost pro zapamatování vybrané akce. Definovanou a uloženou akci naleznete v seznamu známých certifikátů.

Seznam známých certifikátů

Pomocí **seznamu známých certifikátů** můžete přizpůsobit chování ESET Endpoint Antivirus při detekci konkrétních SSL certifikátů. V tomto seznamu naleznete certifikáty, pokud jste ve **Filtrování protokolů SSL/TLS** vybrali **Interaktivní režim**. Seznam naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **SSL/TLS** > **Seznam známých certifikátů**.

Dialogové okno se **seznamem známých certifikátů** obsahuje:

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*. Pomocí tlačítka **Soubor** nahrajete do produktu lokálně uložený certifikát. Pro jeho získání z externího zdroje (online) klikněte na tlačítko **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**.

Seznam SSL/TLS filtrovaných aplikací

Pomocí **seznamu SSL/TLS filtrovaných aplikací** můžete přizpůsobit chování ESET Endpoint Antivirus pro konkrétní aplikace využívající šifrovaný kanál. Do tohoto seznamu se automaticky přidávají také aplikace, pro které jste v **interaktivním režimu** nastavili **zapamatování vybrané akce**. Seznam aplikací naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **SSL/TLS** > **Seznam SSL/TLS filtrovaných aplikací**.

Dialogové okno se **seznamem aplikací**, u kterých je kontrolována SSL/TLS komunikace, obsahuje:

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.

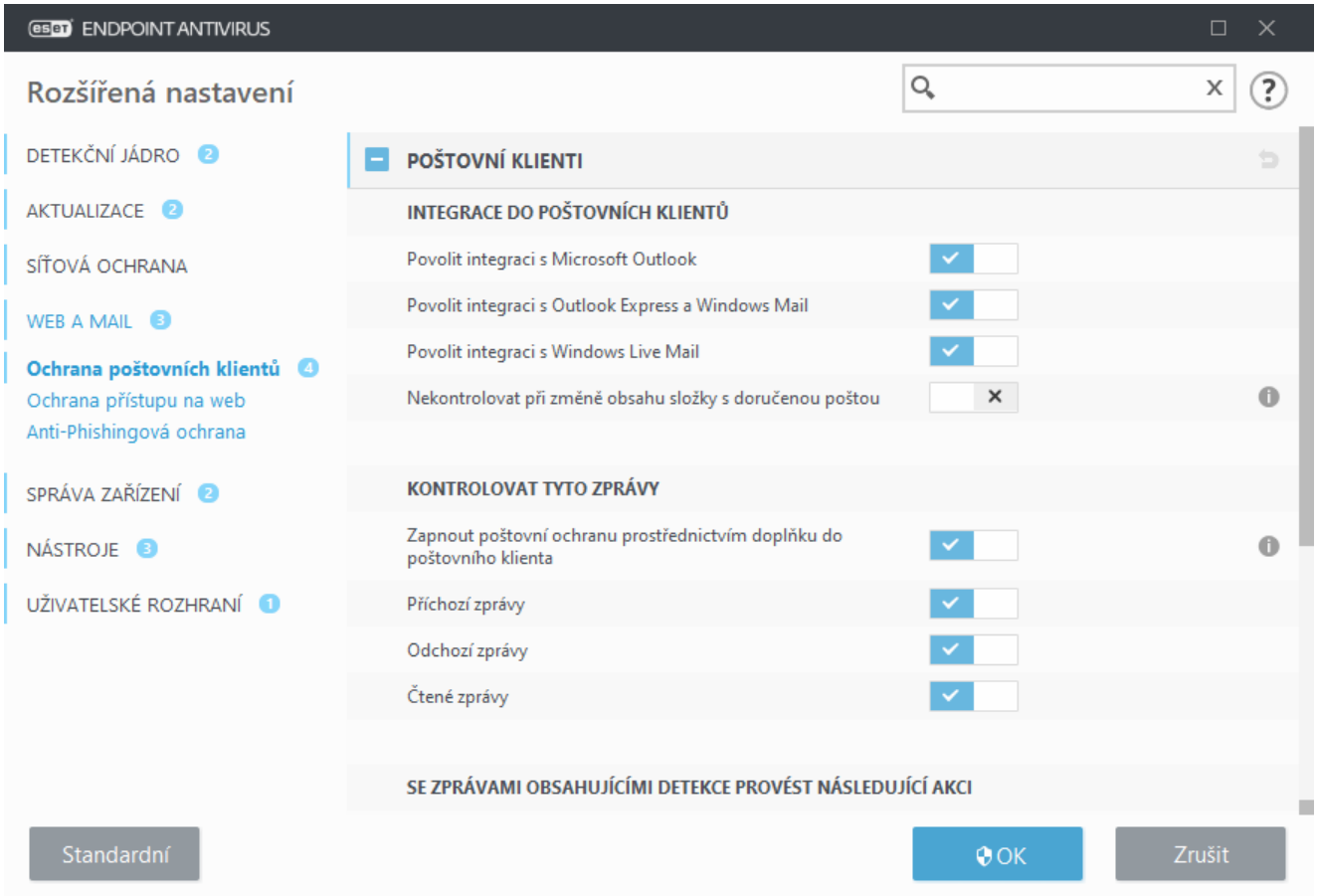
Změnit – vyberte certifikát, který chcete konfigurovat a klikněte na **Změnit**.

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**.

Ochrana poštovních klientů

Integrace ESET Endpoint Antivirus do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdrženým prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET Endpoint Antivirus podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET Endpoint Antivirus do poštovního klienta, což přispívá k efektivnější kontrole e-mailových zpráv. Možnost pro integraci naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **Web a mail** > **Ochrana poštovních klientů** > **Poštovní klienti**.



Kontrolovat tyto zprávy

Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta – vypnutím se deaktivuje ochrana zajišťovaná doplňkem v e-mailových klientech.

Příchozí zprávy – zapnutím povolíte kontrolu přijatých zpráv.

Odchozí zprávy – zapnutím povolíte kontrolu odchozích zpráv.

Čtené zprávy – zapnutím povolíte kontrolu čtených zpráv.

> 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 Filtrováním protokolů (IMAP/IMAPS a POP3/POP3S).

S infikovanými zprávami provést následující akci

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.

Opakovat kontrolu po aktualizaci – zapnutím povolíte opakovanou kontrolu zpráv po aktualizaci detekčního jádra.

Zohlednit výsledky kontroly provedené dalšími moduly – zapnutím umožníte modulu ochrany poštovních klientů zohlednění výsledku kontroly jiným modulem namísto provádění nové kontroly.

Poštovní protokoly

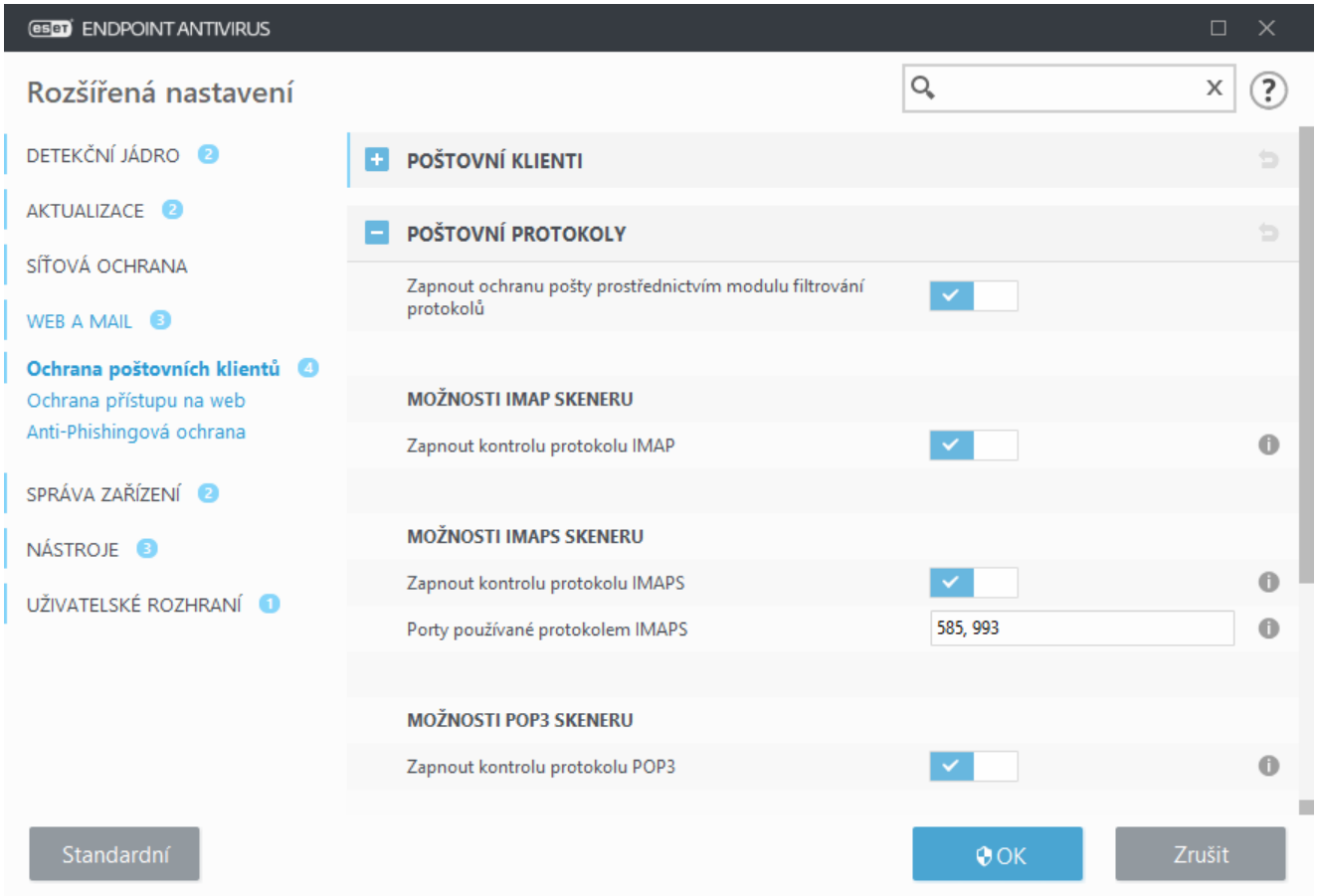
Protokol POP3 a IMAP je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím poštovního klienta. Internet Message Access Protocol (IMAP) je další internetový protokol pro získávání pošty. IMAP má oproti POP3 několik výhod, například více klientů se může současně připojit ke 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 Antivirus 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.

Doporučujeme ponechat možnost **Zapnout ochranu poštovních klientů pomocí filtrování protokolů** zapnutou..Ke konfiguraci kontroly protokolů IMAP/IMAPS a POP3/POP3S přejděte do Rozšířeného nastavení > **Web a mail** > **Ochrana poštovních klientů** > **Poštovní protokoly**.

ESET Endpoint Antivirus rovněž podporuje kontrolu protokolů IMAPS (585, 993) a POP3S (995), které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Endpoint Antivirus kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovat komunikaci na portech definovaných v části **Protokoly používané protokolem IMAPS / POP3S**, bez ohledu na verzi operačního systému. V případě potřeby lze přidat další komunikační porty. Více čísel portů je třeba oddělit čárkou.

Šifrovaná komunikace se standardně nekontroluje. Šifrovaná komunikace (SSL/TLS) je ve výchozím nastavení kontrolována. Pro zobrazení nastavení skeneru přejděte v Rozšířeném nastavení (dostupném po stisknutí klávesy F5 v hlavním okně programu) do sekce **Web a mail** > **SSL/TLS**. Pomocí přepínače **Zapnout filtrování protokolu SSL/TLS** můžete toto chování ovlivnit.



Značení e-mailů

Možnosti konfigurace pro tuto funkci jsou dostupné v **Rozšířeném nastavení (po stisknutí klávesy F5 v hlavním okně) na záložce Web a mail** > **Ochrana poštovních klientů** > **Upozornění a oznámení**.

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. Možná nastavení jsou následující:

- **Nikdy** – program nebude přidávat podpisy do žádných kontrolovaných zpráv,
- **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 odchozích zpráv – vypnutím této funkce se nebude do předmětu infikované zprávy přidávat informace o tom, že obsahuje infiltraci. Tato funkce se dá využít pro snadné filtrování infikovaných zpráv podle předmětu, pokud to poštovní klient umožňuje. Zároveň zvyšuje důvěryhodnost zprávy a v případě výskytu infiltrace nabízí cenné informace o úrovni hrozby pro příjemce i odesílatele.

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 hrozbu.

Integrace do poštovních klientů

Mezi aktuálně podporované poštovní klienty patří Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Ochrana je zajišťována pomocí zásuvného doplňku v těchto programech. 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.

Další nastavení

Optimalizovat zpracování příloh – při vypnutí této možnosti budou všechny přílohy kontrolovány okamžitě. To může mít negativní vliv na výkon e-mailového klienta.

Pokročilé zpracování poštovními klienty – 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 Antivirus se v Microsoft Outlook zobrazí nový panel nástrojů, který obsahuje možnosti antivirové/ ochrany:

ESET Endpoint Antivirus – dvojitým kliknutím na ikonu se otevře program ESET Endpoint Antivirus.

Znovu zkontrolovat zprávy – umožní ruční spuštění kontroly e-mailů. Zde můžete nastavit zprávy, které budou zkontrolovány, a můžete aktivovat opakovanou kontrolu přijatého e-mailu. Více informací naleznete v kapitole ochrana poštovních klientů.

Možnosti skeneru – otevře okno s nastavením ochrany poštovních klientů.

Panel nástrojů v Outlook Express a Windows Mail

Ochrana Outlook Express and Windows Mail pracuje jako zásuvný modul (plug-in). Po instalaci ESET Endpoint Antivirus se v Microsoft Outlook zobrazí nový panel nástrojů, který obsahuje možnosti antivirové/ ochrany:

ESET Endpoint Antivirus – dvojitým kliknutím na ikonu se otevře program ESET Endpoint Antivirus.

Znovu zkontrolovat zprávy – umožní ruční spuštění kontroly e-mailů. Zde můžete nastavit zprávy, které budou zkontrolovány, a můžete aktivovat opakovanou kontrolu přijatého e-mailu. Více informací naleznete v kapitole ochrana poštovních klientů.

Možnosti skeneru – otevře okno s nastavením ochrany poštovních klientů.

Uživatelské rozhraní

Přizpůsobit vzhled – umožňuje upravit vzhled panelu nástrojů. Zrušením této možnosti se vzhled panelu nástrojů přizpůsobí podle nastavení poštovního klienta.

Zobrazit text – u ikon se zobrazí text s popisem.

Text vpravo – text s popisem se zobrazí vpravo vedle ikony.

Velké ikony – na panelu nástrojů se zobrazí velké ikony.

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 Antivirus 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.

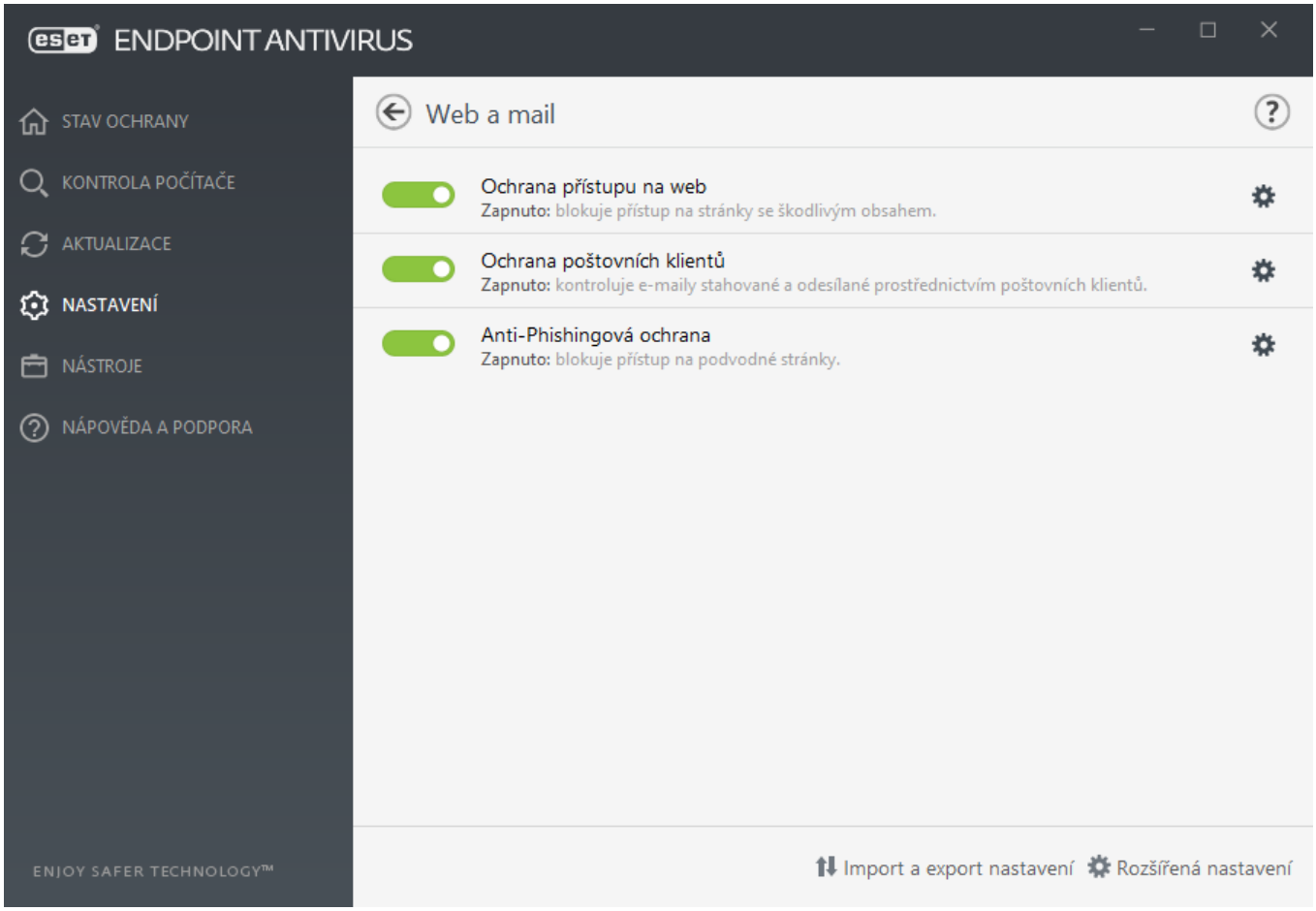
Možnost **Kontrolovat zprávy, které již byly překontrolovány** zajistí nové zkontrolování zpráv, které již byly v minulosti zkontrolovány.

Ochrana přístupu na web

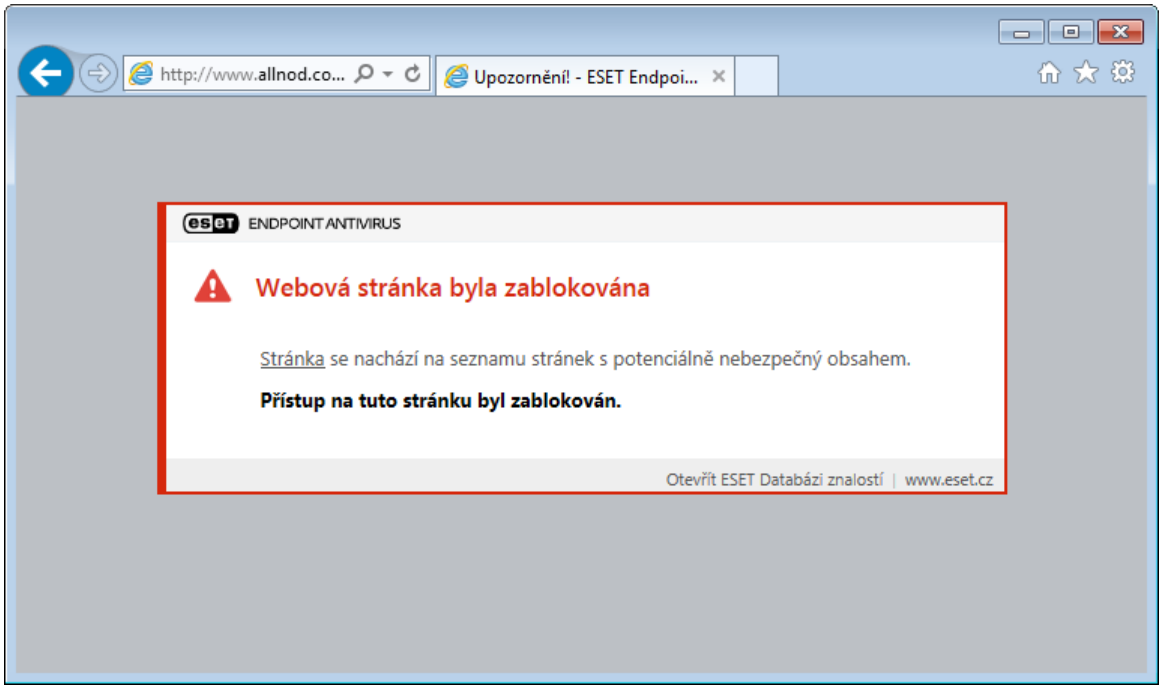
Internetové připojení se stalo u počítačů standardem. Bohužel i pro šíření škodlivého kódu. Ochrana přístupu na web monitoruje komunikaci mezi webovým prohlížečem a vzdáleným serverem, kdy filtruje HTTP (Hypertext Transfer Protocol) a HTTPS (šifrovanou komunikaci) na základě pravidel.

Přístup na známé webové stránky se škodlivým obsahem je zablokován ještě předtím, než je škodlivý kód stažen do počítače. Všechny ostatní webové stránky budou zkontrolovány skenovacím jádrem ThreatSense při svém načtení a zablokovány při zjištění škodlivého obsahu. K dispozici jsou dva režimy ochrany přístupu na web, blokování na základě seznamu blokovaných adres a blokování na základě obsahu.

Důrazně doporučujeme mít funkci Ochrana přístupu na web zapnutou. Možnosti konfigurace této funkce naleznete v hlavním okně programu ESET Endpoint Antivirus na záložce **Nastavení** > **Internetová ochrana** > **Ochrana přístupu na web**.



Při přístupu na blokovanou stránku se v internetovém prohlížeči zobrazí níže uvedená zpráva:

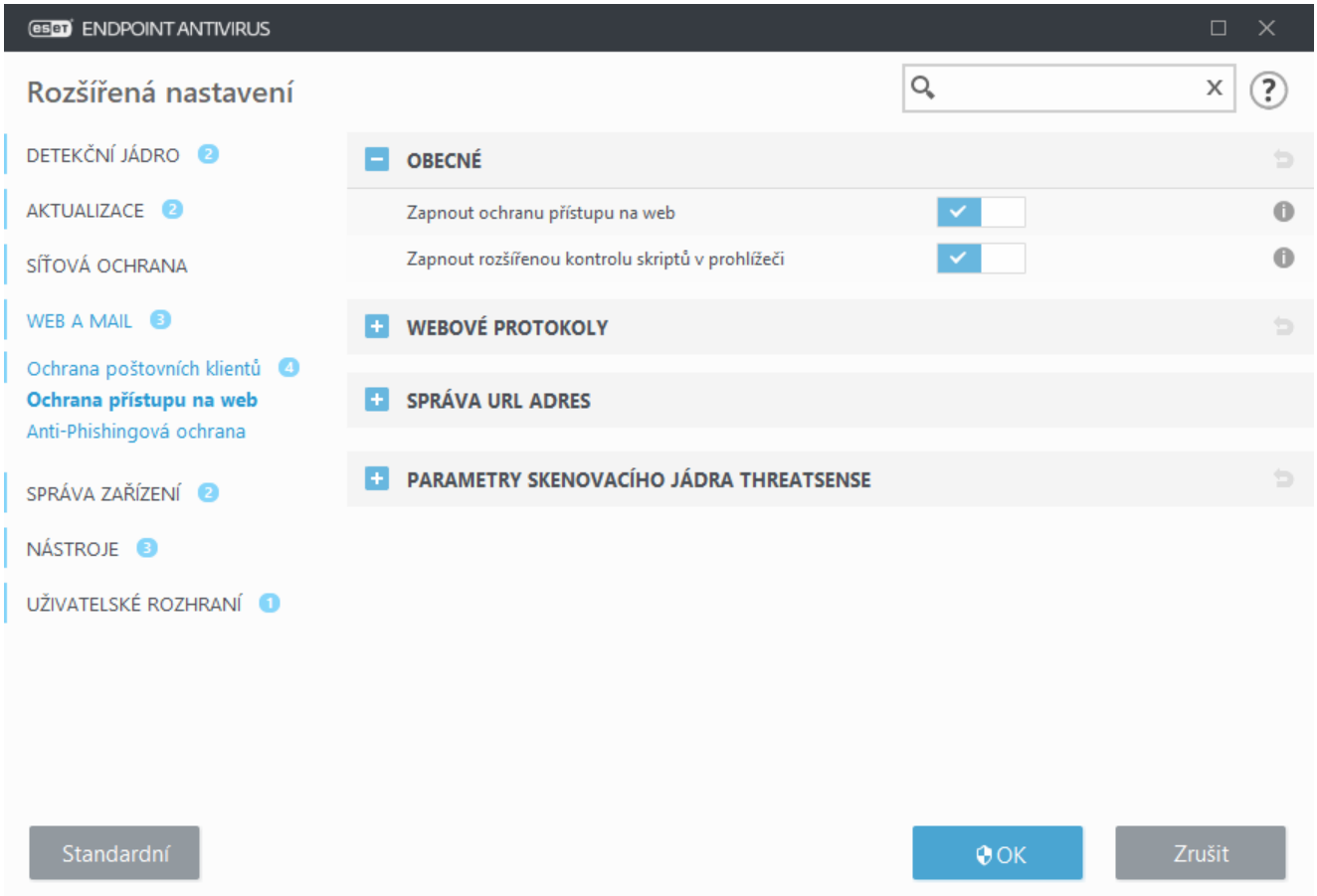


Následující články z ESET Databáze znalostí mohou být dostupné pouze v angličtině:

- Jak odblokovat přístup na bezpečnou stránku přímo v ESET Endpoint Antivirus

Podrobné možnosti konfigurace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně) na záložce **Web a mail** > **Ochrana přístupu na web**. Zde nastavte následující možnosti:

- **Obecné** – v této části máte možnosti pro zapnutí nebo vypnutí této funkce.
- **Webové protokoly** – v této části můžete definovat monitorování standardních protokolů používaných internetovými prohlížeči.
- **Správa URL adres** – v této části můžete definovat seznamy adres webových stránek, které chcete blokovat, povolit nebo vyloučit z kontroly obsahu.
- **Parametry skenovacího jádra ThreatSense** – nabízí pokročilé nastavení kontroly, jako jsou cíle kontroly (e-maily, archivy aj.), metody detekce ochrany přístupu na web apod.



Rozšířená nastavení Ochrany přístupu na web

Podrobné možnosti konfigurace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně) na záložce **Web a mail** > **Ochrana přístupu na web** > **Obecné**:

Zapnout ochranu přístupu na web – pokud je tato možnost vypnutá, nebude funkční Ochrana přístupu na web ani Anti-Phishingová ochrana.

Zapnout rozšířenou kontrolu skriptů v prohlížeči – pokud je tato možnost zapnutá, automaticky bude detekční jádro kontrolovat všechny JavaScript programy spuštěné internetovými prohlížeči.

V rámci zajištění bezpečnosti nedoporučujeme ochranu přístupu na web vypínat.

Webové protokoly

Standardně je ESET Endpoint Antivirus nakonfigurován tak, aby monitoroval HTTP protokol používaný nejrozšířenějšími internetovými prohlížeči.

Nastavení skeneru HTTP

HTTP komunikace je vždy monitorována na všech portech a ve všech aplikacích.

Nastavení skeneru HTTPS

ESET Endpoint Antivirus také podporuje kontrolu protokolu HTTPS. ESET Endpoint Antivirus podporuje rovněž kontrolu protokolů HTTPS, které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Endpoint Antivirus kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovat pouze komunikaci na portech (443, 0-65535) definovaných v **Portech používaných protokolem HTTPS** bez ohledu na verzi operačního systému.

Šifrovaná komunikace se standardně nekontroluje. Šifrovaná komunikace (SSL/TLS) je ve výchozím nastavení kontrolována. Pro zobrazení nastavení skeneru přejděte v Rozšířeném nastavení (dostupném po stisknutí klávesy F5 v hlavním okně programu) do sekce **Web a mail** > **SSL/TLS**. Pomocí přepínače **Zapnout filtrování protokolu SSL/TLS** můžete toto chování ovlivnit.

Správa URL adres

V sekci Správa URL adres můžete definovat HTTP adresy, které chcete blokovat, povolit nebo vyloučit z kontroly obsahu.

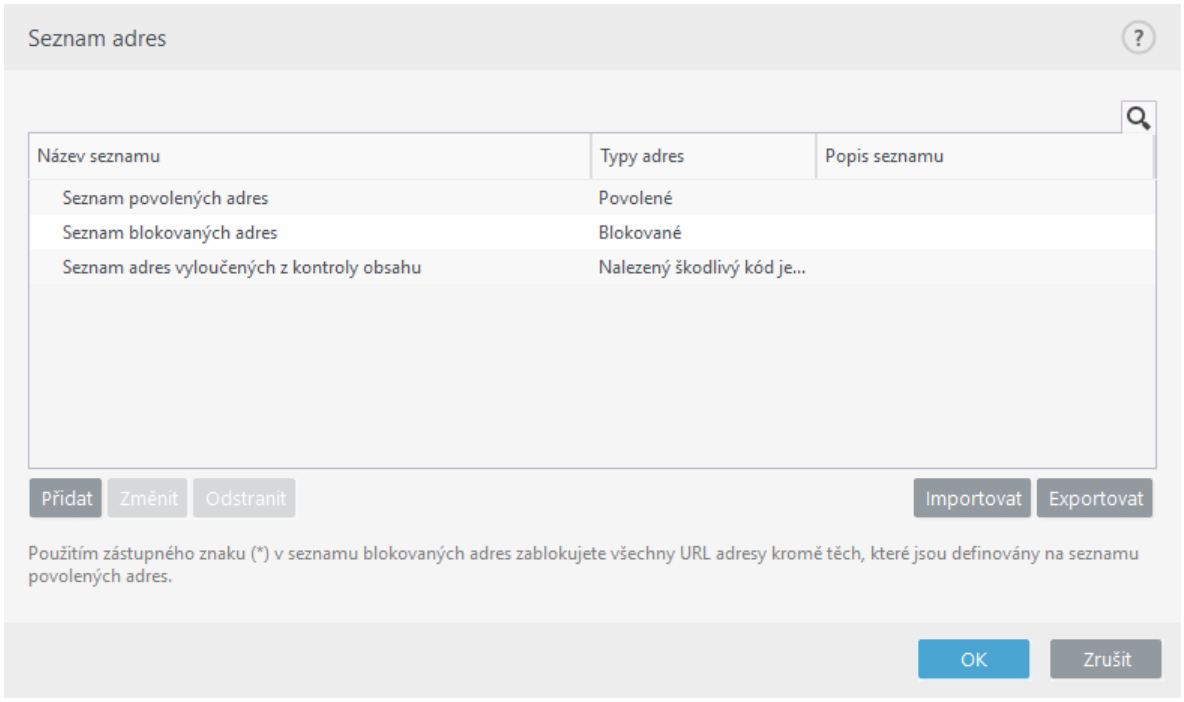
Možnost **Zapnout filtrování protokolu SSL/TLS** musí být aktivní, pokud chcete filtrovat HTTPS adresy současně HTTP. V opačném případě by byl zakázán pouze přístup na nešifrovanou HTTPS verzi webové stránky.

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**.

Pokud máte aktivní možnost **Nekontrolovat komunikaci s důvěryhodnými doménami** (v sekci **Web a mail** > **SSL/TLS**, komunikace s těmito doménami bude automaticky vyloučena z kontroly.



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.

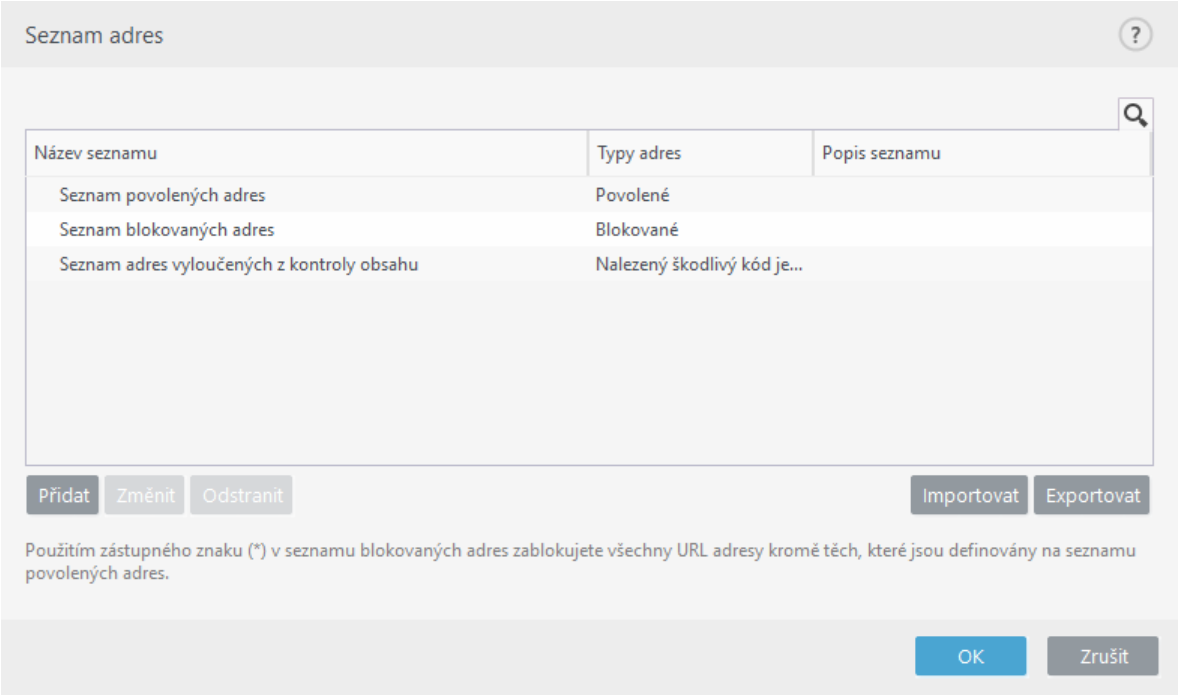
Seznam adres

V této části můžete definovat seznamy adres, které budou blokovány, povoleny, nebo vyloučeny z kontroly na přítomnost škodlivého kódu.

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 Antivirus

Pro více informací přejděte do kapitoly Správa URL adres.

Vytvoření nového seznamu

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 Antivirus 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/*

Anti-Phishingová ochrana

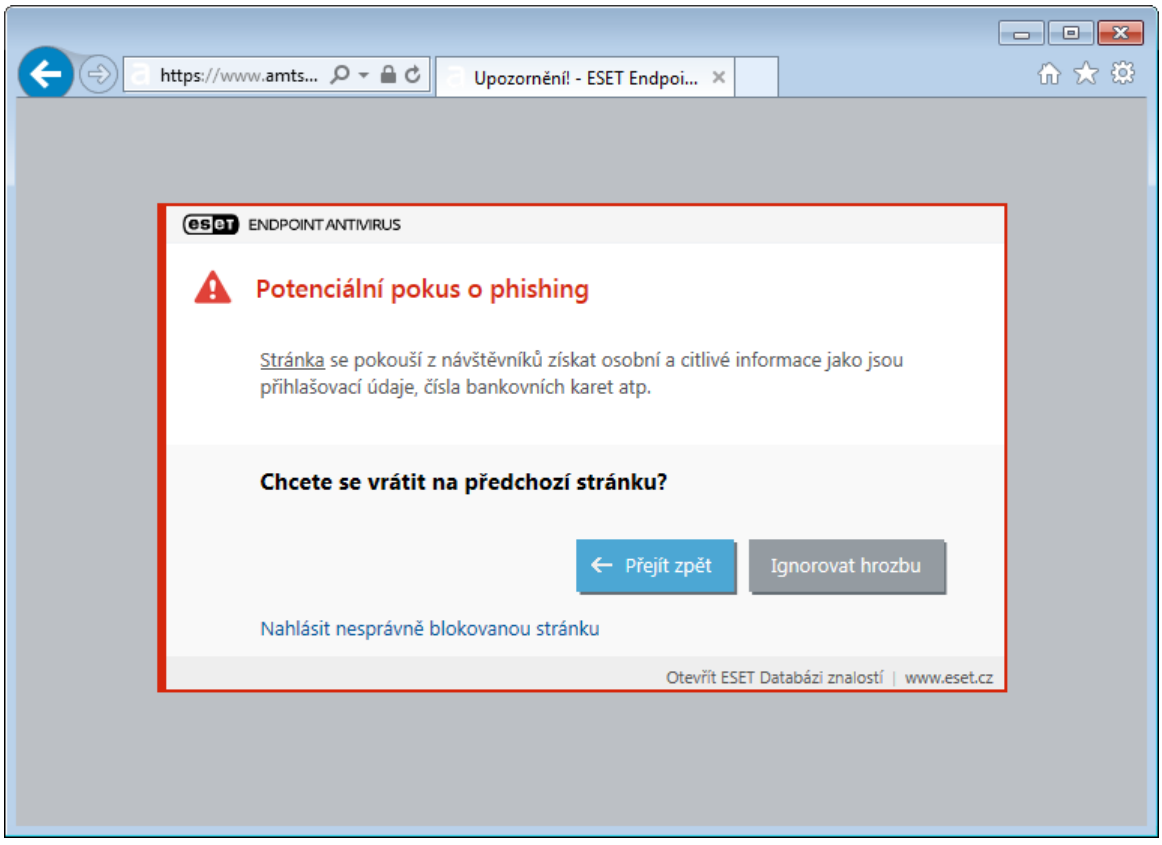
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem útočníků využívajících phishing je získání citlivých dat, jako jsou čísla bankovních účtů, PIN kódy a další. Více informací naleznete v glosáři. ESET Endpoint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

Anti-Phishingová ochrana je ve výchozím nastavení zapnutá. Podrobné možnosti konfigurace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Anti-Phishingová ochrana**.

Podrobnější informace o fungování Anti-Phishingové ochrany ESET Endpoint Antivirus 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. Pokud chcete trvale povolit přístup na danou stránku, použijte Správce URL adres – v **Rozšířeném nastavení** přejděte na záložku **Web a mail** > **Ochrana přístupu na web** > **Správa URL adres** a na řádku **Seznam adres** klikněte na **Změnit**.

Nahlášení phishingové stránky

Pokud narazíte na stránku se škodlivým obsahem, zašlete prosím daný odkaz k analýze do virové laboratoře ESET prostřednictvím této stránky.

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 použijte tento odkaz.

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.).

Aktualizace programu

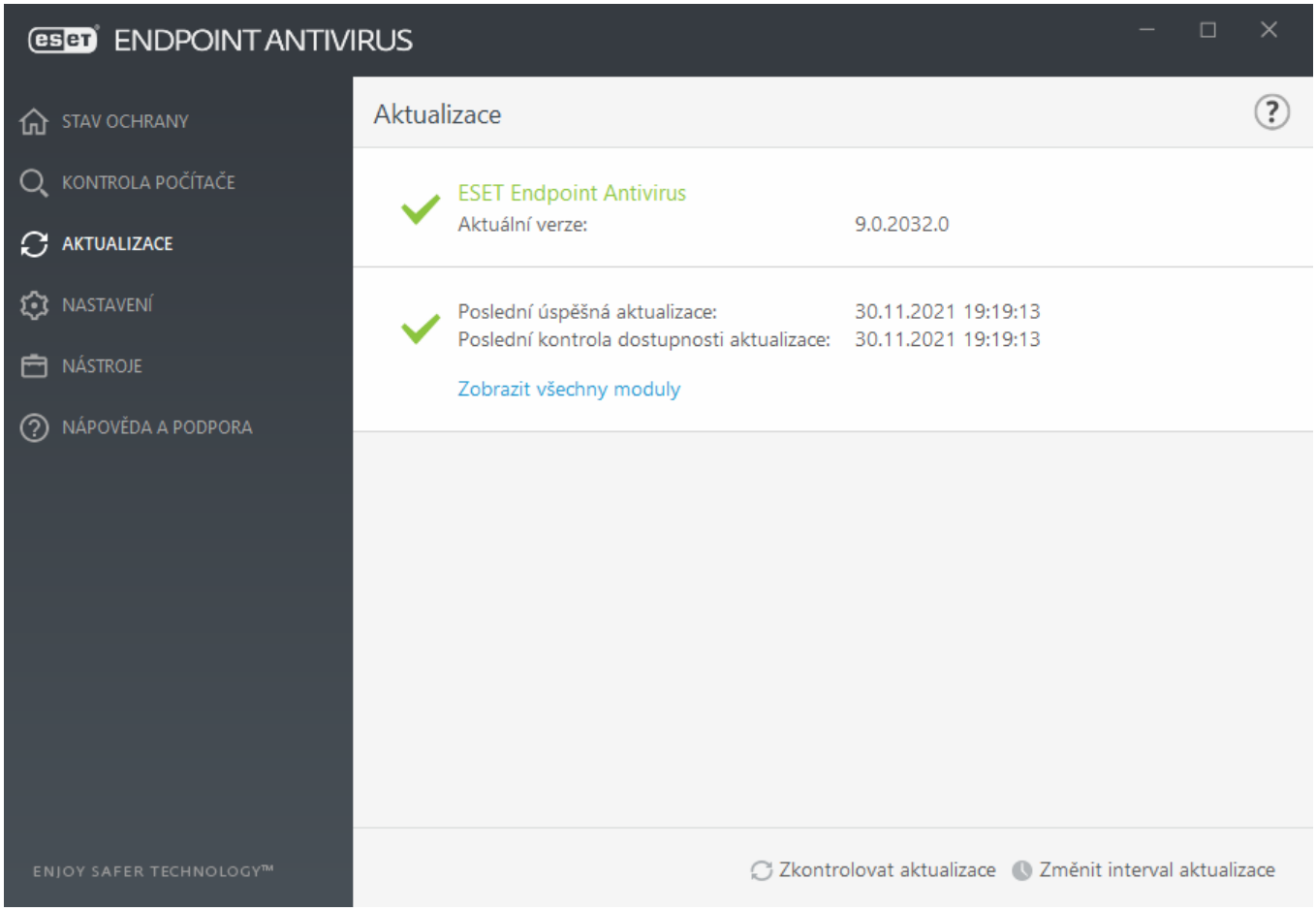
Pravidelná aktualizace programu ESET Endpoint Antivirus je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program používal nejnovější detekční jádro a programové moduly. Aktualizace probíhá automaticky po aktivování produktu.

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. Kliknutím na **Zobrazit všechny moduly** otevřete dialogové okno se seznamem všech používaných modulů společně s informacemi o jejich verzi.

Jejich dostupnost můžete kdykoli ověřit kliknutím na tlačítko **Zkontrolovat aktualizace**. Pro správnou funkčnost programu a ochranu proti škodlivému software je nezbytné aktualizovat detekční jádro a programové moduly. Věnujte pozornost konfiguraci a průběhu aktualizací. Pokud jste produkt do této chvíle neaktivovali, budete k tomu vyzváni. Po kliknutí na tlačítko **Aktivovat produkt** zadejte licenční klíč.

Pokud jste ESET Endpoint Antivirus 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.

Licenční klíč jste obdrželi po nákupu nebo registraci ESET Endpoint Antivirus. informací navštivte ESET Databázi znalostí.



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

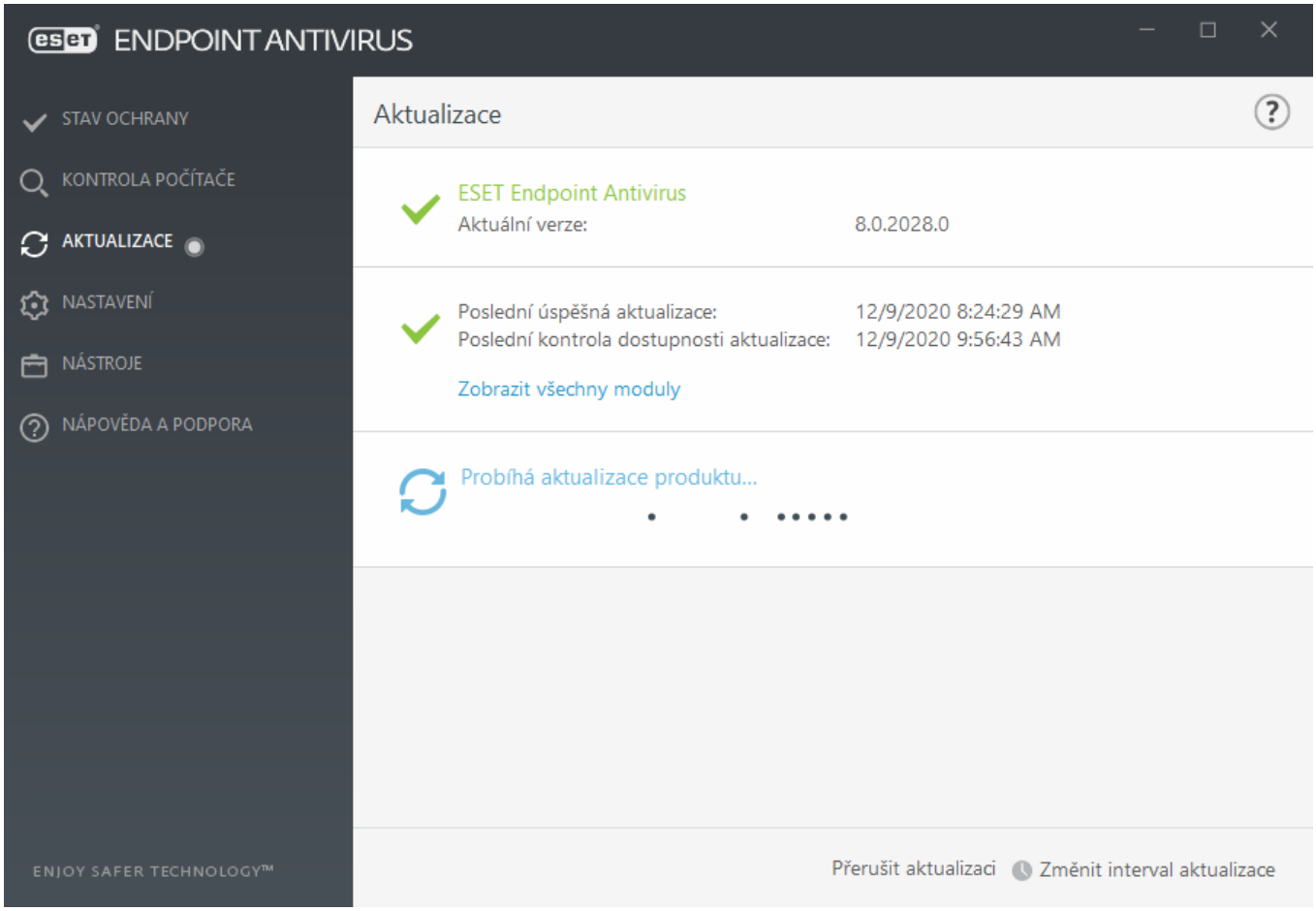
Poslední úspěšná aktualizace – zobrazuje datum, kdy se program naposledy úspěšně aktualizoval. Pokud nevidíte dnešní datum, detekční jádro nemusí být aktuální.

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.

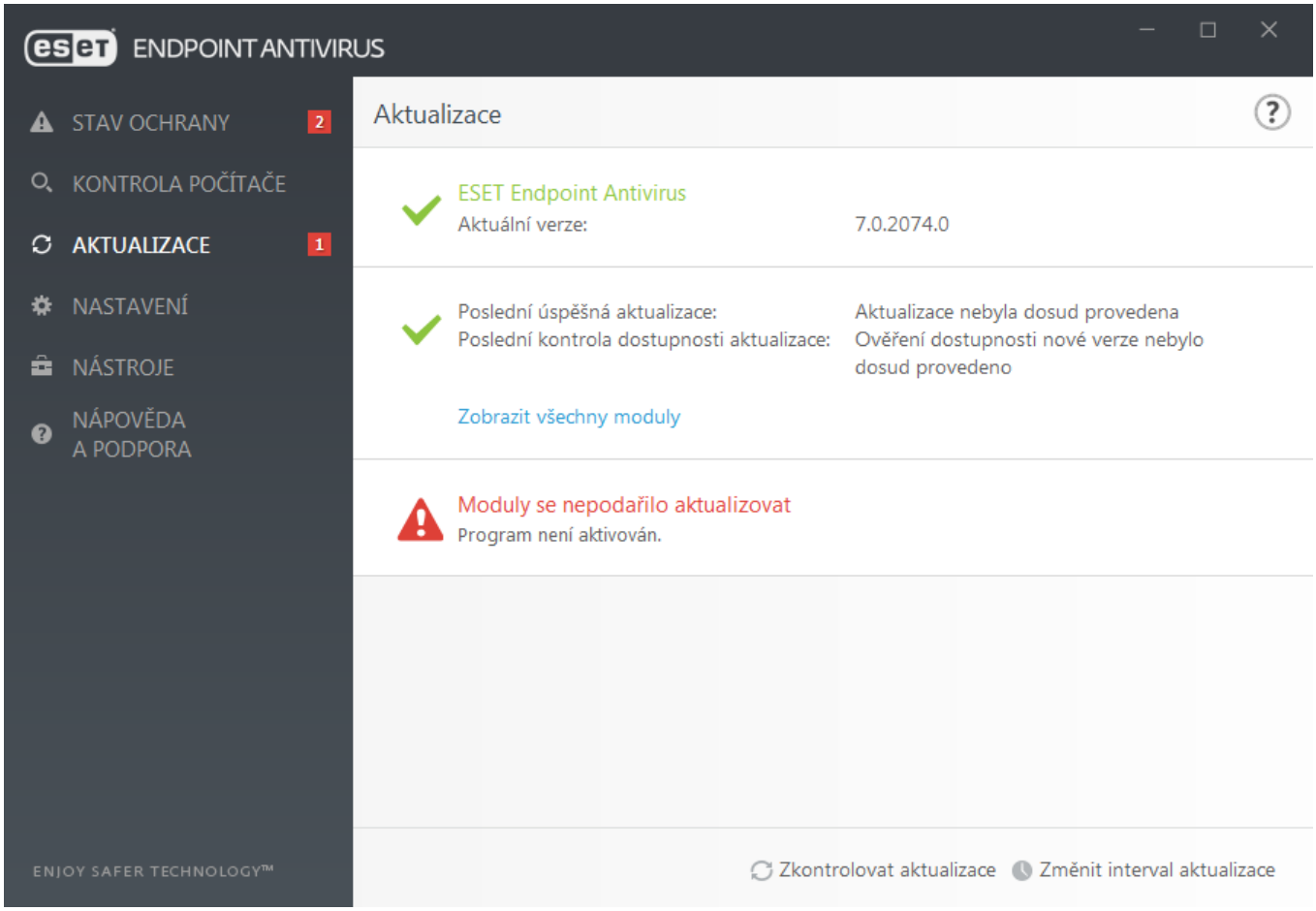


Za normálních okolností se modul aktualizuje několikrát denně. Pokud tomu tak není, program není aktualizován a zvyšuje se riziko infiltrace. V opačném případě se zobrazí jedno z následujících oznámení:

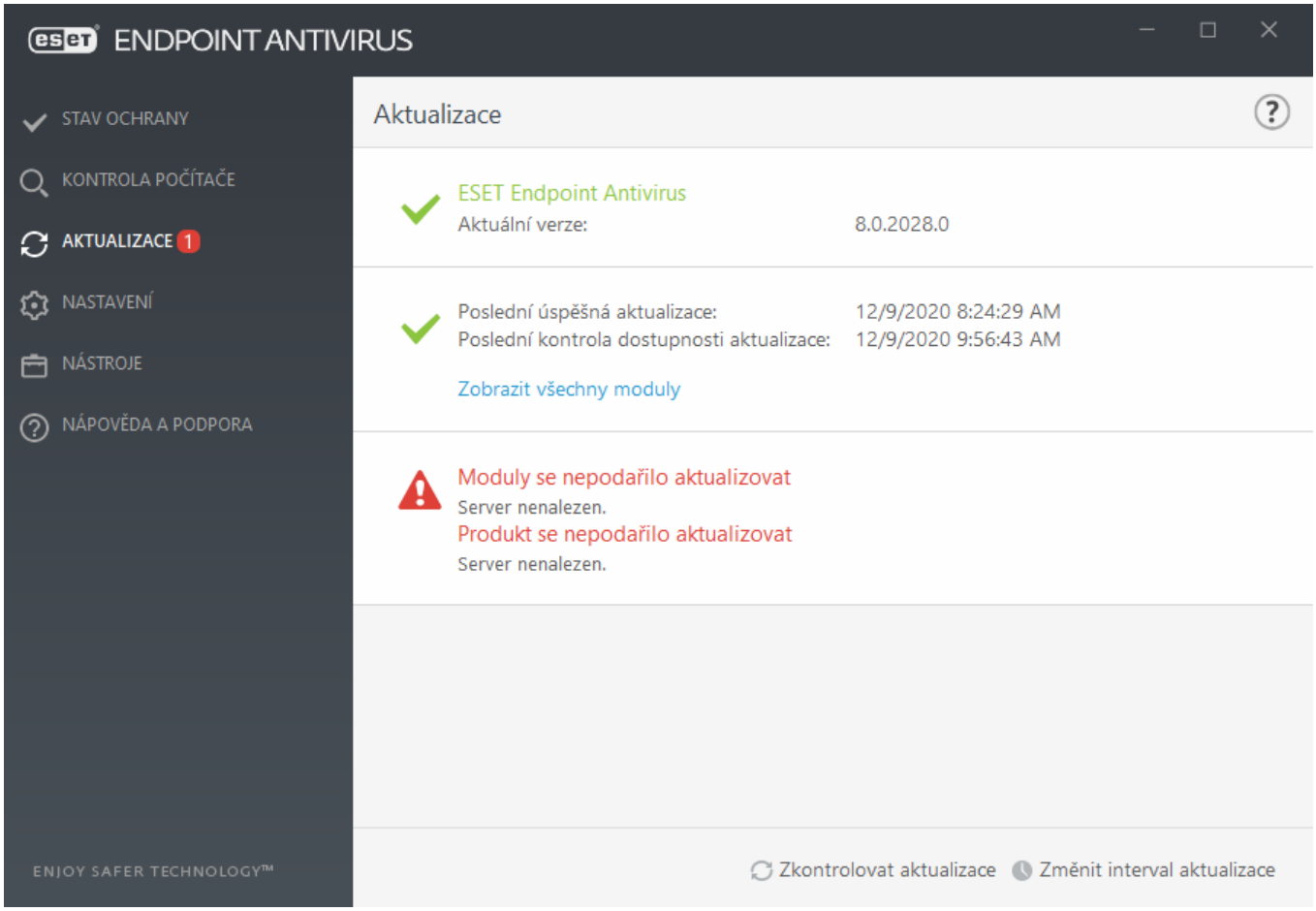
Detekční jádro není aktuální – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci modulů. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Mezi nejčastější důvody patří nesprávně zadaná ověřovací data nebo nesprávně nastavené připojení k internetu.

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

1. **Neplatný licenční klíč** – v hlavním okně program přejděte na záložku Nápověda a podpora, zde klikněte na tlačítko Změnit licenci. V dialogovém okně klikněte na příslušnou nabídku. Běžně stačí kliknout na nabídku Použít zakoupený licenční klíč a tento do okna zadat. Volbu potrvďte kliknutím na **Pokračovat**.



2. **Chyba při stahování aktualizačních souborů** – při pokusu o stažení aktualizačních souborů došlo k chybě. Chyba může souviset s nesprávným nastavením připojení k internetu. Doporučujeme zkontrolovat připojení k internetu (otevřením jakékoliv webové stránky ve webovém prohlížeči). Rovněž doporučujeme zkontrolovat, zda je počítač připojen k internetu, a ověřit, zda poskytovatel internetu nemá výpadek připojení.



Pro více informací navštivte ESET Databázi znalostí.

Nastavení aktualizace

Možnosti aktualizace jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **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 povolen přístup k internetu (například HTTPS komunikaci).

Obecné

Aktuálně používaný aktualizační profil se zobrazuje v rozbalovacím menu **Vyberte výchozí profil aktualizace**.

Pro vytvoření nového profilu přejděte do kapitoly Profily.

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.

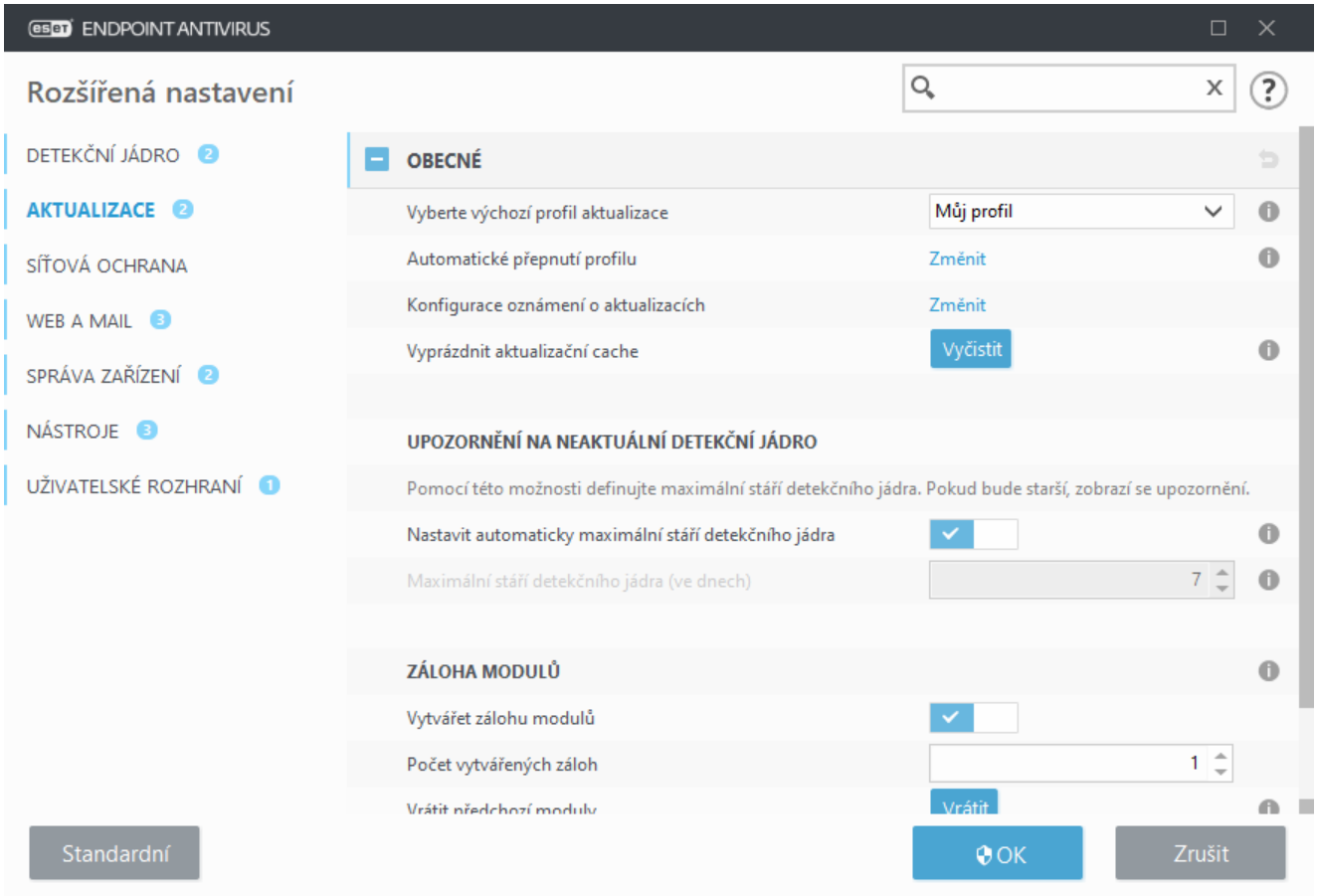
Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit** na řádku **Vyprázdnit aktualizační cache**.

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**.

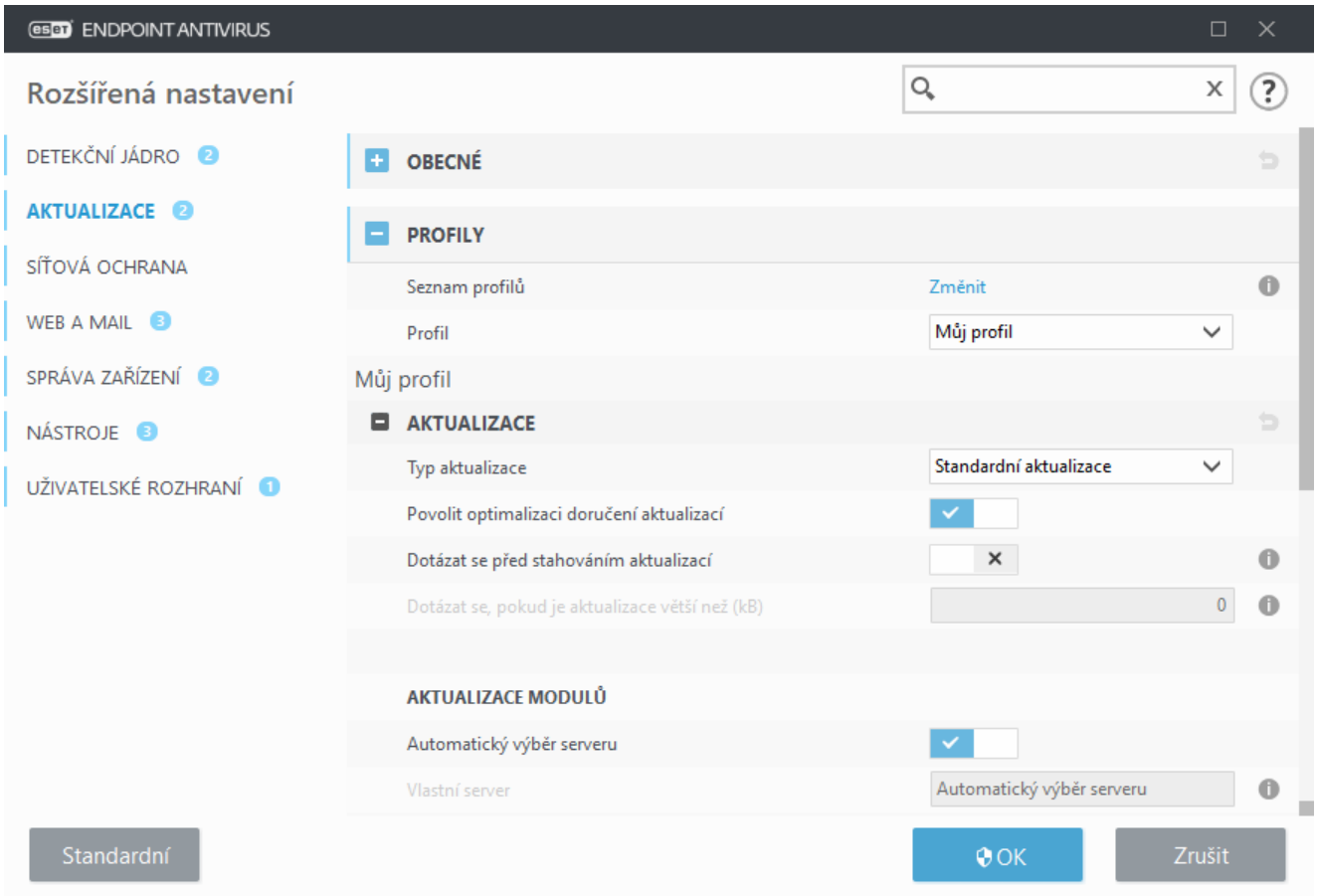
Pro vytvoření nového klikněte na **Změnit** vedle položky **Seznam profilů**, následně klikněte na tlačítko **Přidat** a zadejte **Název profilu**.

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. Vyberete-li možnost Opožděné aktualizace, aktualizace se budou stahovat z aktualizačního severu, na který jsou aktualizace umisťovány 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.

Aktualizace 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.

Aktualizační mirror

Pro více informací přejděte do kapitoly Aktualizační mirror.

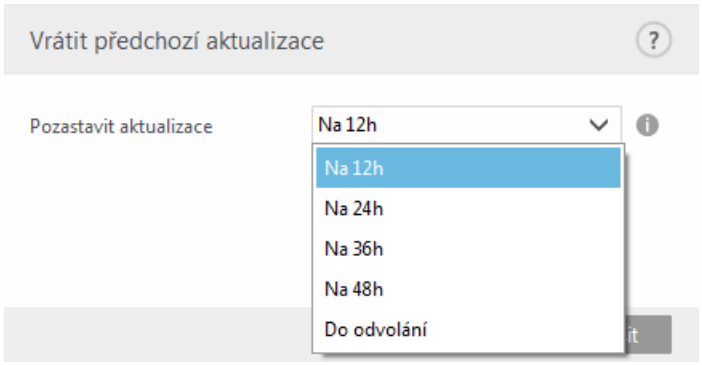
Obnovení předchozí verze modulů

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 Antivirus 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.

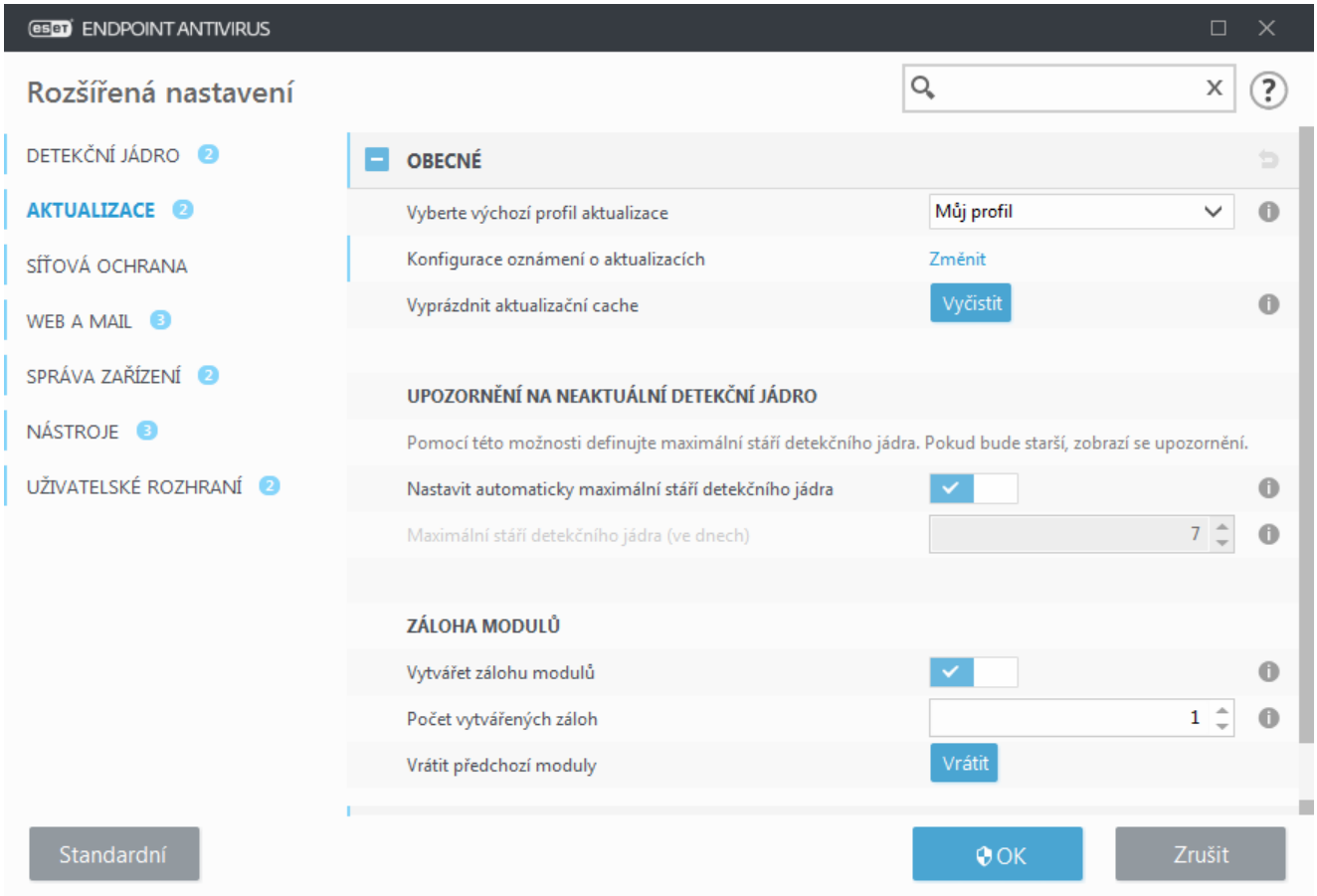
Při dosažení maximálního počtu vytvářených záloh (například tří), dojde každých 48 hodin k nahrazení nejstarší zálohy novou. ESET Endpoint Antivirus se při obnovení předchozí verze detekčního jádra a programových modulů vrátí vždy k nejstarší verzi.

Pokud kliknete na tlačítko **Vrátit** (v **Rozšířeném nastavení** (F5) > **Aktualizace** > **Obecné**), vyberte z rozbalovacího menu **časový interval**, na jak dlouho chcete aktualizaci detekčního jádra a programových modulů pozastavit.



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 obnovní 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 Antivirus.

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

Pro přístup k nastavení proxy serveru pro daný aktualizační profil přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) do sekce **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 definovaná v **Rozšířeném nastavení** v sekci **Nástroje** > **Proxy server**.

Pomocí možnosti **Nepoužívat proxy server** zajistíte, aby se při aktualizaci ESET Endpoint Antivirus nepoužíval

proxy server.

Možnost **Připojení prostřednictvím proxy serveru** vyberte v případě, že:

- Pro aktualizaci ESET Endpoint Antivirus 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 Antivirus 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. V tomto případě dejte pozor na to, aby měl daný uživatelský účet měl práva pro přístup do složky s aktualizačními soubory na serveru. 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.

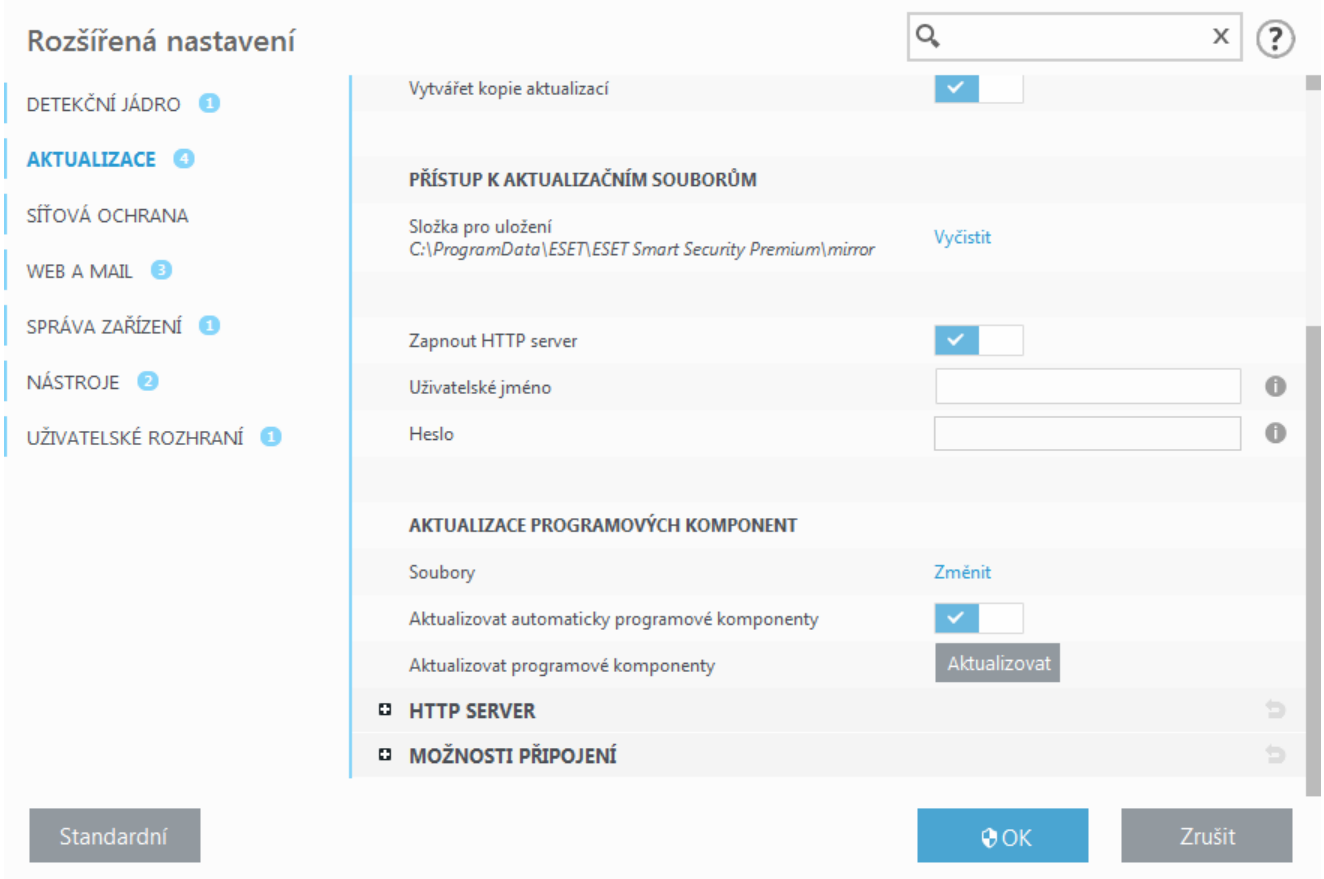
Po dokončení aktualizace **odpojit** ze serveru – pokud aktivujete tuto možnost, po dokončení aktualizace se vynutí ukončení spojení se serverem.

Aktualizační mirror

ESET Endpoint Antivirus 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 zajistí snížení zátěže na připojení k internetu.

Ve velkých sítích, kde je pro správu používán ESET PROTECT, doporučujeme pro minimalizaci množství stahovaných dat z internetu upřednostnit Apache HTTP Proxy před konfigurací mirroru na některém z klientů. Apache HTTP Proxy můžete nainstalovat společně s ESET PROTECT prostřednictvím all-in-one instalačního balíčku nebo ji nasadit jako samostatnou komponentu. Pro více informací a přehled rozdílů mezi Apache HTTP Proxy, nástrojem Mirror Tool a přímým spojením přejděte do Online nápovědy k ESET PROTECT.

Možnosti konfigurace lokálního mirroru naleznete v **Rozšířeném nastavení** v sekci Aktualizace. V hlavním okně programu stiskněte klávesu **F5** a následně přejděte do sekce **Aktualizace** > **Profily** rozbalte část **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 Antivirus\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.

Zpřístupnění mirroru prostřednictvím lokálního HTTP serveru

Je použito automaticky jako předdefinované nastavení, při standardní instalaci. Proto pro zpřístupnění mirroru pomocí HTTP serveru stačí v **Rozšířeném nastavením** (dostupném po stisknutí klávesy F5 v hlavním okně programu) přejít na záložku **Aktualizace** > **Profily** > **Aktualizační mirror** a aktivovat 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 Antivirus 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 přejděte do **Rozšířeného nastavení** a v sekci **Aktualizace** > **Profily**> **Aktualizační mirror** 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 si **Rozšířená nastavení** (F5) a přejděte do sekce **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 Antivirus).

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** (**F5**) produktu ESET Endpoint Antivirus 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 ESET Endpoint Antivirus 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/era6`

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 Antivirus 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 Antivirus 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, že jsou údaje zadány 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 Antivirus nenaváže spojení k mirroru – není povolena komunikace na portu, na kterém běží HTTP server.

ESET Endpoint Antivirus zahlásí chybu při stahování aktualizačních souborů – nejčastěji jde o chybnou konfiguraci aktualizačního serveru (síťové cesty ke složce s mirrorem).

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**. Standardně jsou v ESET Endpoint Antivirus již vytvořeny tyto aktualizační úlohy:

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

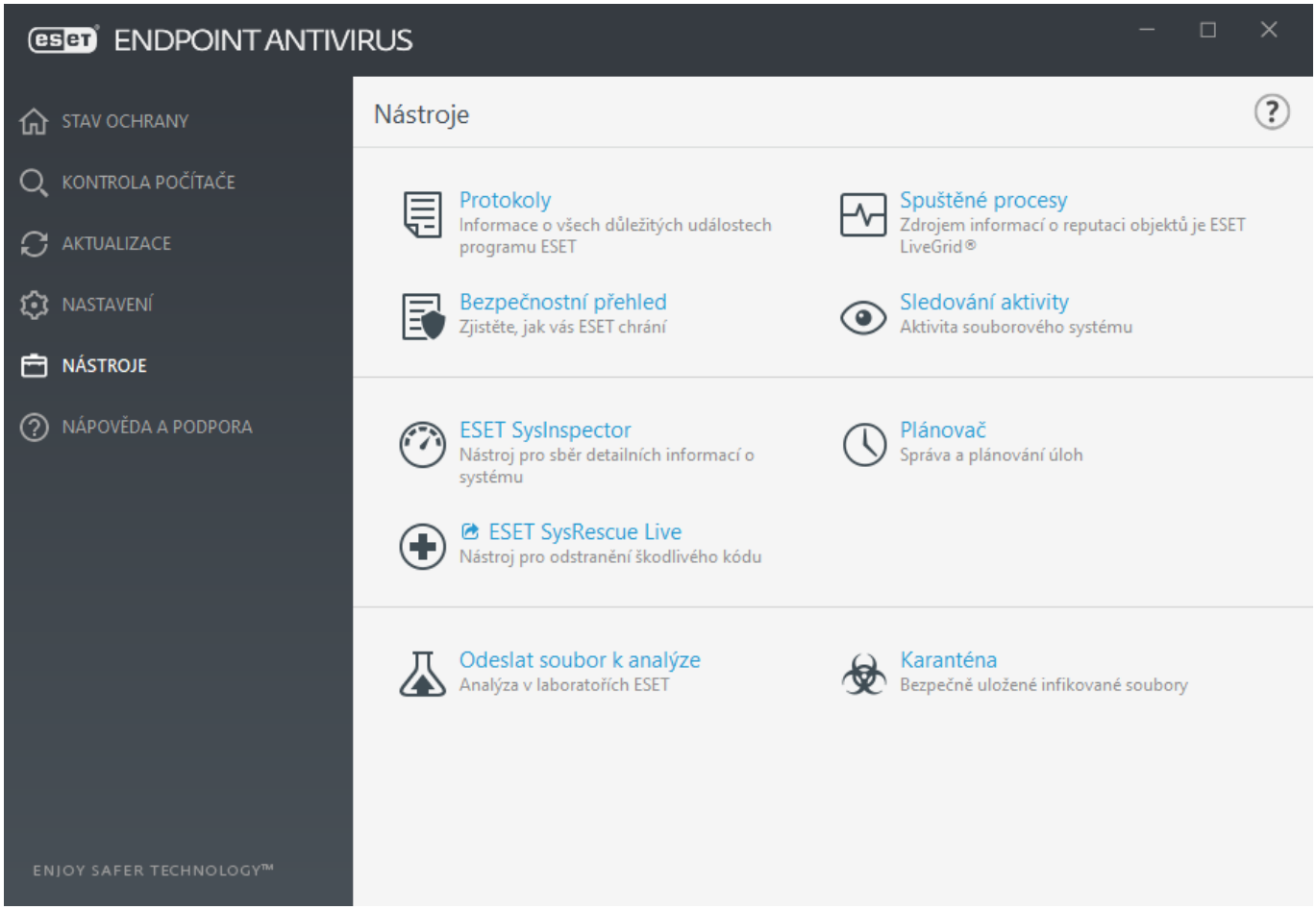
Každou z uvedených aktualizačních úloh můžete upravit podle svých představ. Kromě standardních aktualizačních úloh můžete vytvořit nové aktualizační úlohy s vlastním nastavením. Podrobněji se vytváření a nastavení aktualizačních úloh zabýváme v kapitole Plánovač.

Nástroje

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

V této sekci naleznete následující nástroje:

- Protokoly
- Spuštěné procesy (tato součást se dostupná, pokud máte v produktu ESET Endpoint Antivirus aktivní technologii ESET LiveGrid®)
- Bezpečnostní přehled (v nespravovaných prostředích)
- ESET SysInspector
- Plánovač
- ESET SysRescue Live – přesměruje vás na webové stránky nástroje ESET SysRescue Live, kde si můžete stáhnout přímo .iso obraz pro vytvoření záchranného ESET SysRescue Live CD/USB.
- Odeslat soubor k analýze – umožní odeslat podezřelý soubor k analýze do virové laboratoře ESET (v závislosti na nastavení ESET LiveGrid® nemusí být možnost povolená).
- 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 informace a protokoly si můžete prohlédnout přímo v prostředí ESET Endpoint Antivirus. 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:

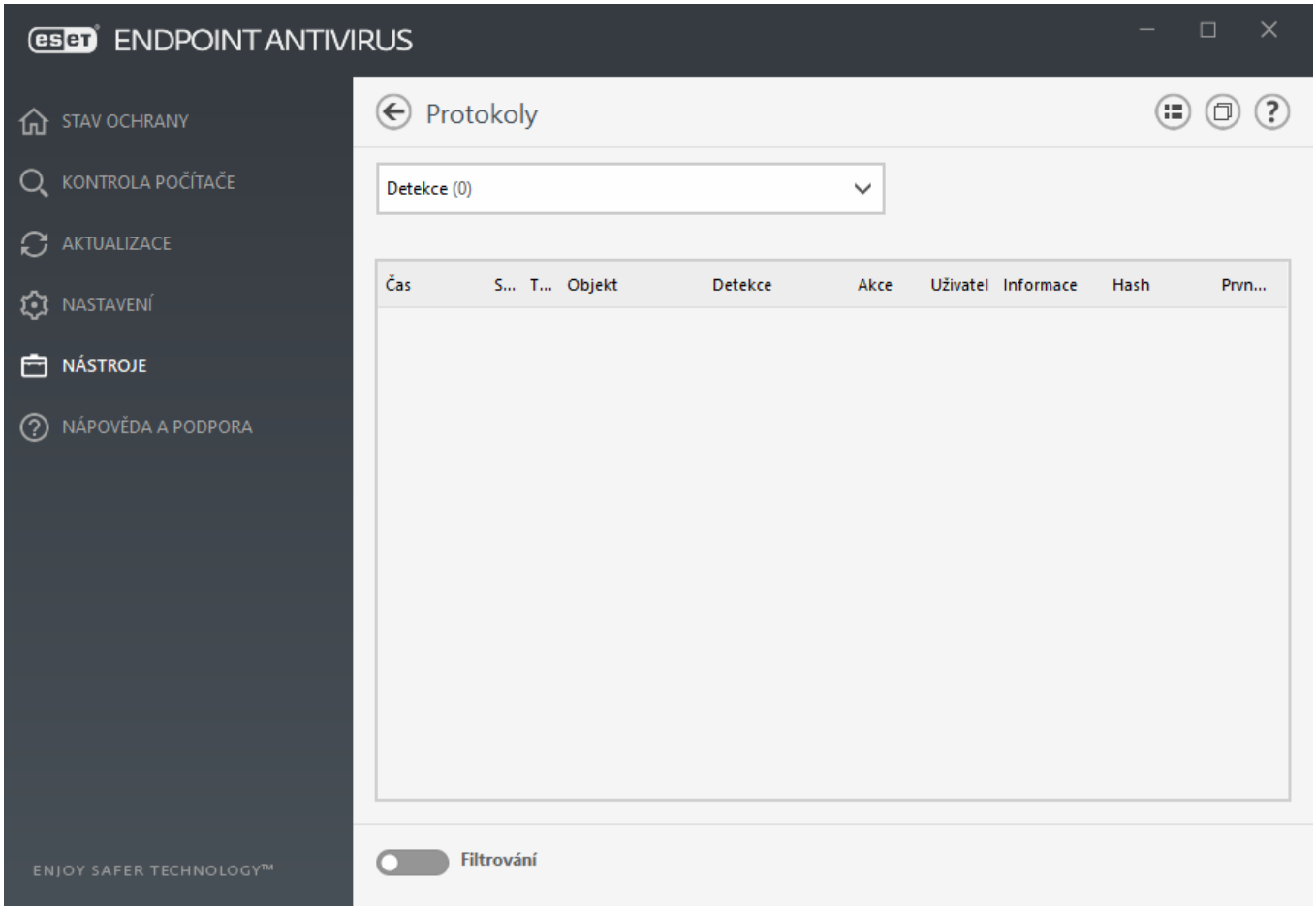
- **Detekce** – protokol zachycených detekcí a infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly programu ESET Endpoint Antivirus. Informace zahrnují čas detekce, název infiltrace, umístění, provedenou činnost a uživatele přihlášeného v době detekce. Dvojklikem na záznam 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 Antivirus 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 uživatelské příručky 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
- **Síťová ochrana** – protokol obsahuje všechny vzdálené útoky zachycené ochranou proti síťovým útokům. 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 rozšířená nastavení.

- **Filtrované webové stránky** – Tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem Ochrana přístupu na web. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.

- **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.
- **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 se otevře dialogové Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů.
- **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. Takový zúžený počet záznamů oceníte, pokud hledáte konkrétní typ události, stav nebo určité 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** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy,
- **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.

Konfigurace protokolování

Nastavení protokolování produktu ESET Endpoint Antivirus je přístupné z hlavního okna programu. Přejděte na záložku **Nastavení** a klikněte na **Rozšířená nastavení** > **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** – zaznamenány budou 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 atd.).

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.

Audit

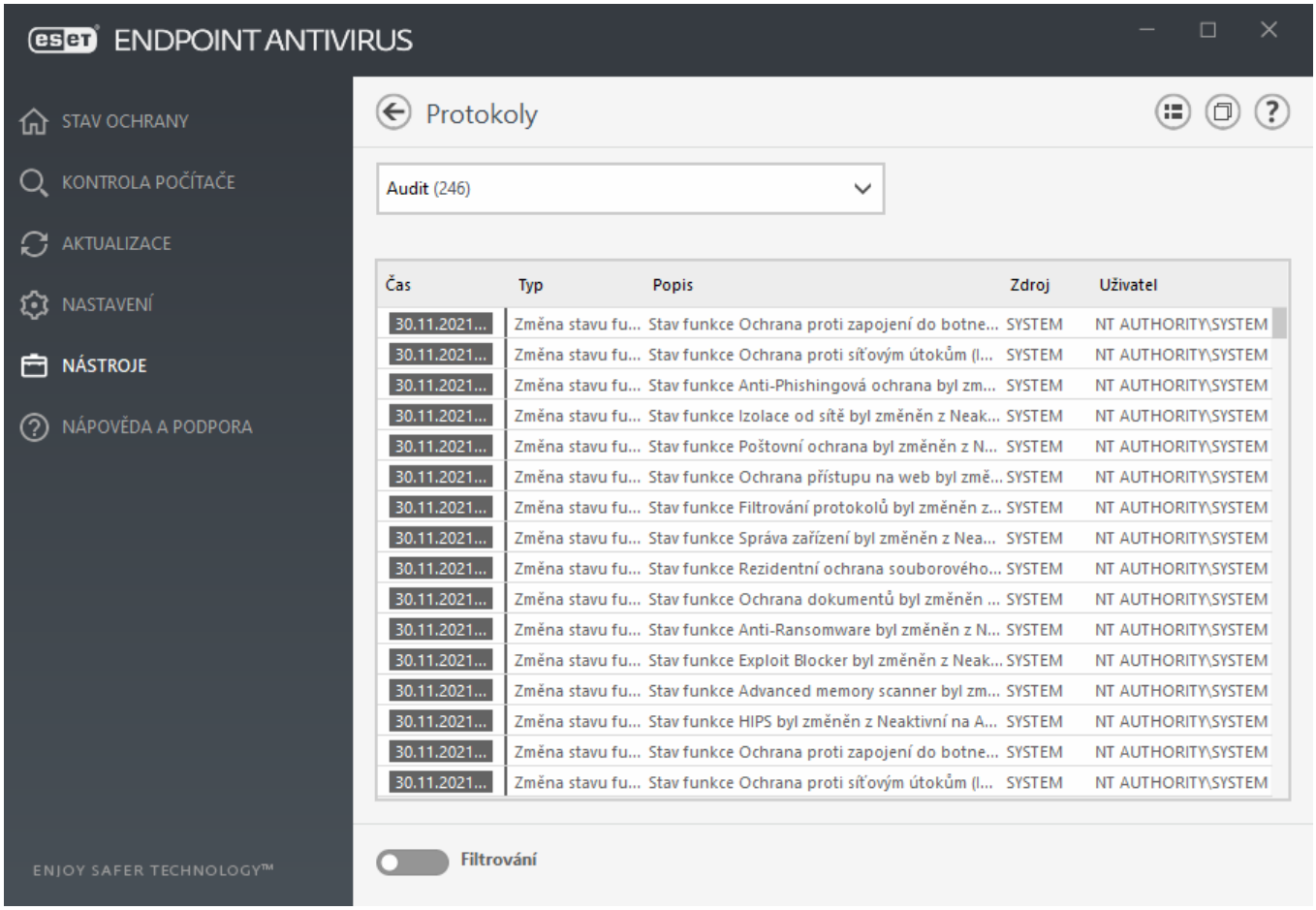
V enterprise prostředích má obvykle více uživatelů oprávnění pro konfiguraci bezpečnostních produktů. Protože změna konfigurace produktu může mít dramatický dopad na jeho fungování, je nezbytné, aby administrátoři měli k dispozici přehled o provedených změnách, který by mohli použít pro rychlou identifikaci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

Audit log představuje nový typ protokolování dostupný v ESET Endpoint Antivirus od verze 7.1. 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.

Plánovač

spravuje a spouští naplánované úlohy s nastavenými parametry a vlastnostmi.

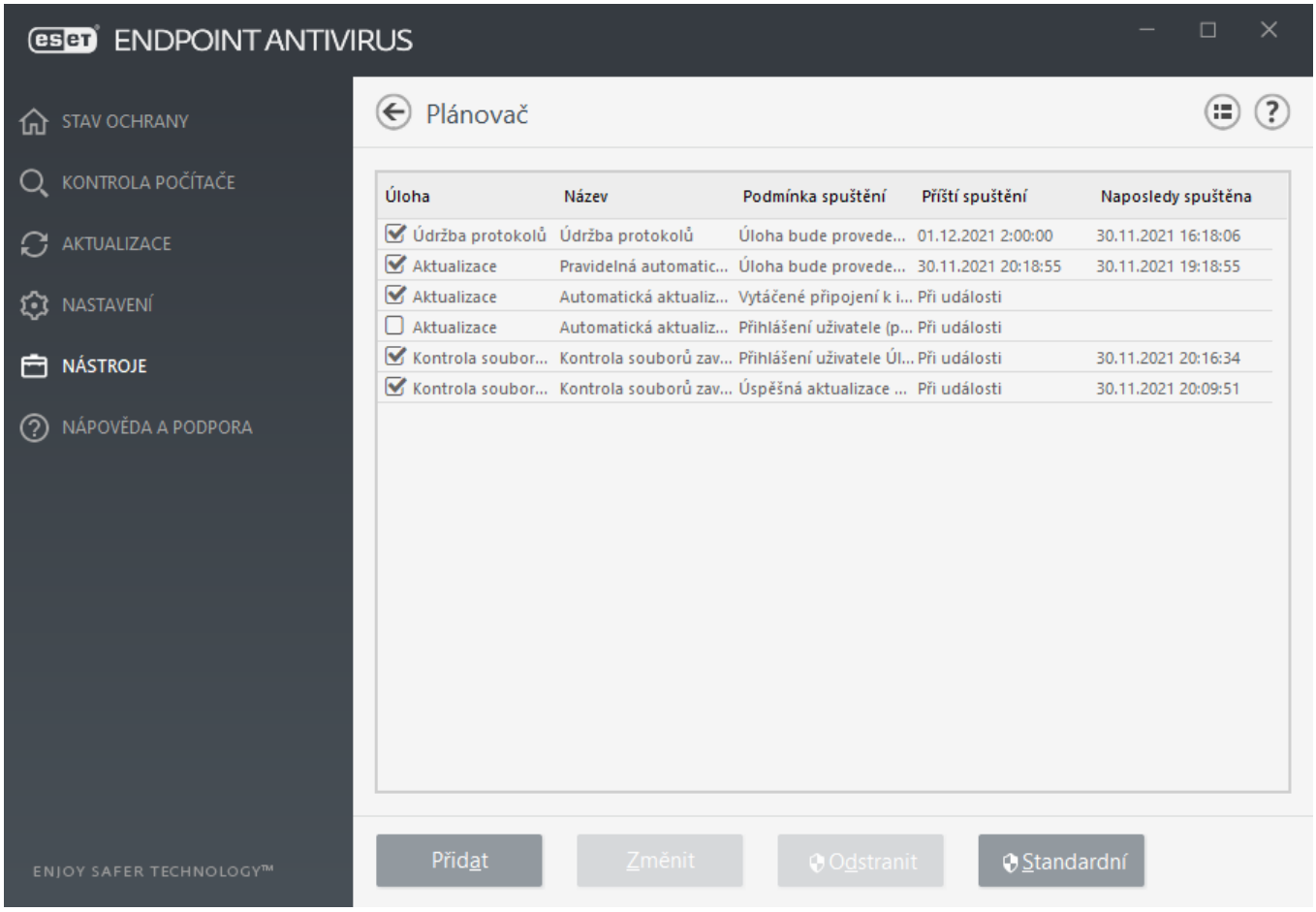
Plánovač je dostupný v hlavním okně programu ESET Endpoint Antivirus na záložce **Nástroje** > Plánovač. Plánovač obsahuje seznam všech naplánovaných úloh a jejich nastavení jako je datum a čas provedení, použitý profil kontroly atp.

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. V kontextovém menu, které se zobrazí po kliknutí pravým tlačítkem myši v okně plánovače, jsou dostupné akce pro: zobrazení detailních informací o úloze, okamžité provedení úlohy, vytvoření nové úlohy, úpravu resp. 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),

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**.



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. Tyto informace mohou být užitečné při zjišťování příčiny podezřelého chování systému ať už vlivem nekompatibility software/hardware nebo infekce škodlivého kódu. Více informací naleznete v online uživatelské příručce k nástroji ESET SysInspector.

V okně 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** – kliknutím si zobrazíte vybraný vytvořený 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**).
- **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** – odstraní vybraný protokol,
- **Odstranit vše** – vybráním této možnosti odstraníte všechny protokoly.
- **Exportovat…** – po vybrání této možnosti uložíte protokol do .XML souboru nebo do zazipovaného .XML souboru.

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.

Na výběr máte ze tří možností:

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 Antivirus 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 Antivirus 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 Antivirus máme k dispozici v Databázi znalostí v angličtině několika dalších jazycích.

Konfigurace cloudové ochrany v Rozšířeném nastavení produktu

Pro přístup ke konfiguraci ESET LiveGrid® stiskněte v hlavním okně programu klávesu **F5** a v Rozšířeném nastavení přejděte do sekce **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.

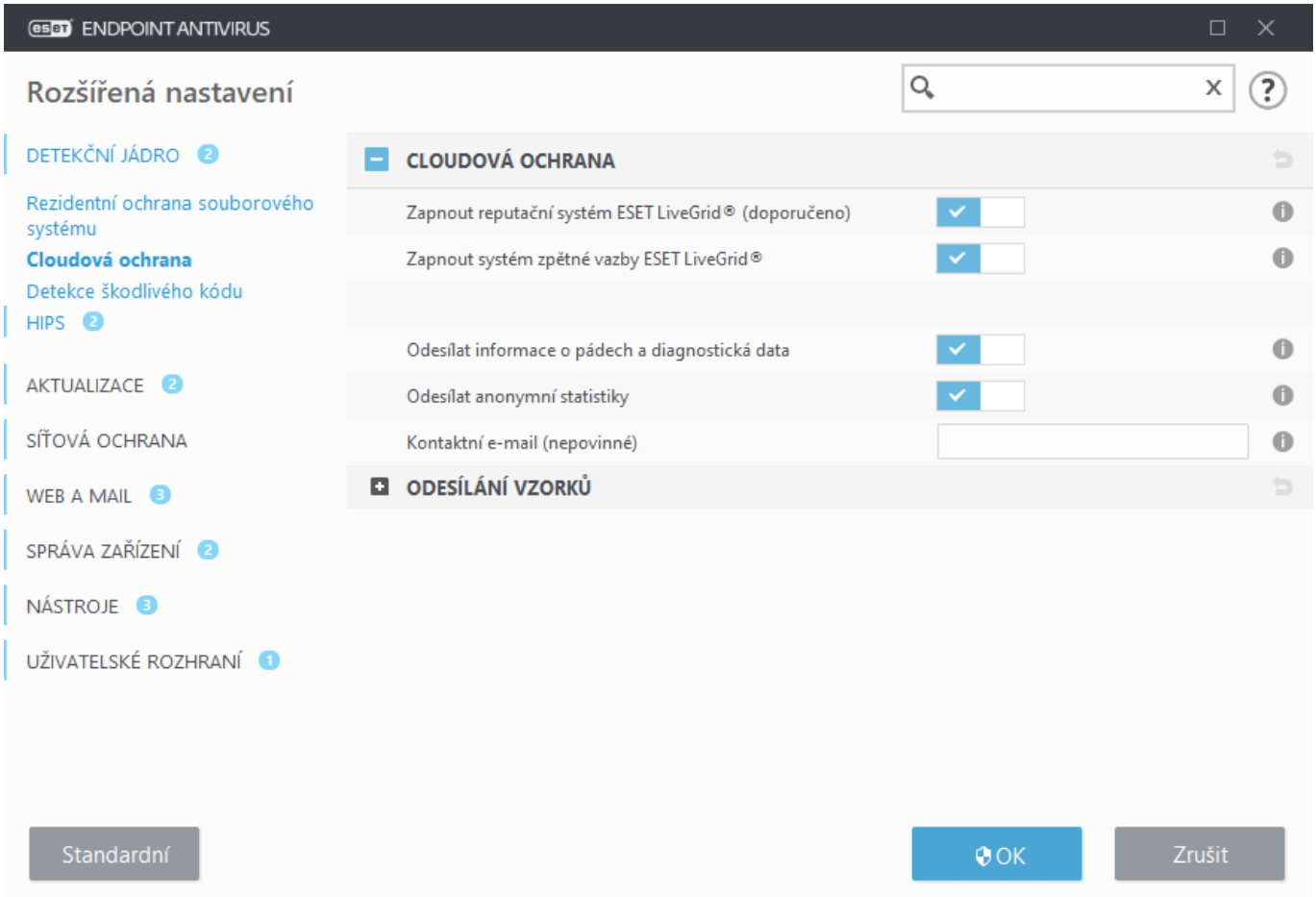
Zapnout systém zpětné vazby ESET LiveGrid® – po aktivování se budou do laboratoří ESET k analýze odesílat relevantní data (popsáno níže v sekci **Odesílání vzorků**) společně se statistikami a hlášeními o pádech.

Zapnout ESET LiveGuard (tato možnost není dostupná přímo v produktu ESET Endpoint Antivirus) – 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. Prosím, mějte na paměti, že od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.



Odesílání vzorků

Ruční odesílání vzorků – pomocí této možnosti povolíte ruční odeslání vzorku k analýze do společnosti ESET z kontextového menu, karantény nebo sekce Nástroje > Odeslat soubor k analýze.

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 Antivirus 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 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 a definujte výjimku následovně: *download.domain.com*.

ESET LiveGuard

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

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

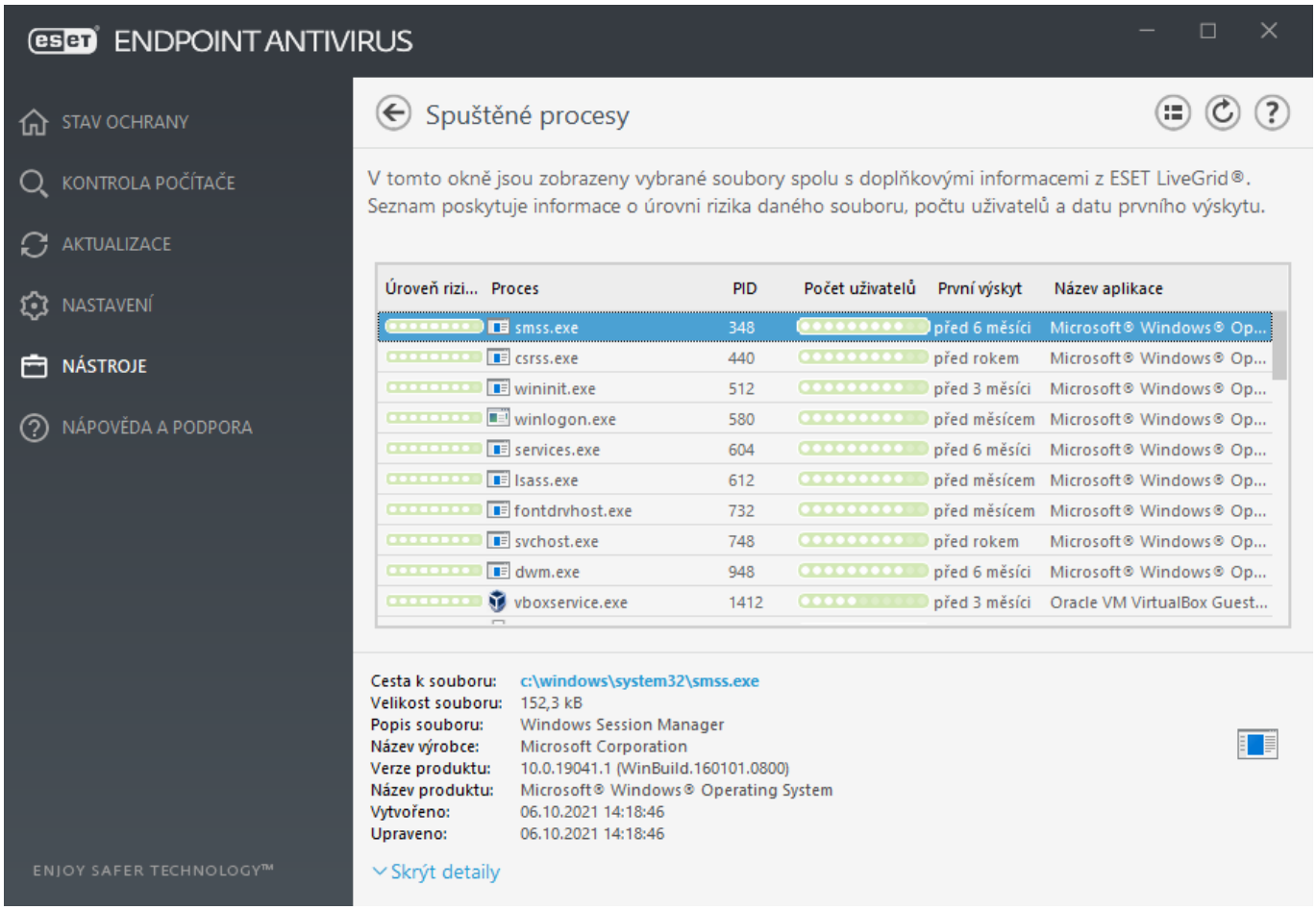
Pomocí seznamu výjimek můžete zabránit v odesílání konkrétních typů souborů nebo obsahu složek k analýze. Soubory uvedené na seznamu nebudou nikdy odeslány do laboratoří ESET k analýze, i pokud by se v nich nacházel škodlivý kód. Standardně se neodesílají nejrozšířenější typy souborů (.doc, atp.).

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 a definujte výjimku následovně: *download.domain.com*.

Spuštěné procesy

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



Reputace – ve většině případů přiřazuje ESET Endpoint Antivirus 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®.

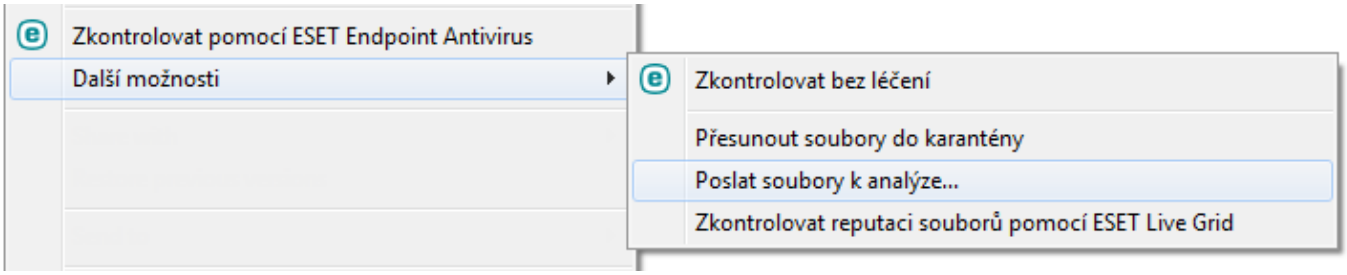
> I v případě, že je aplikace označená jako Neznáma (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete soubor odeslat k analýze do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde o aplikaci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

Detekované PUA – zobrazuje počet detekovaných potenciálně nechtěných aplikací (PUA).

Zkontrolováno dokumentů – zobrazuje počet zkontrolovaných dokumentů.

Zkontrolováno aplikací – zobrazuje počet zkontrolovaných spustitelných objektů.

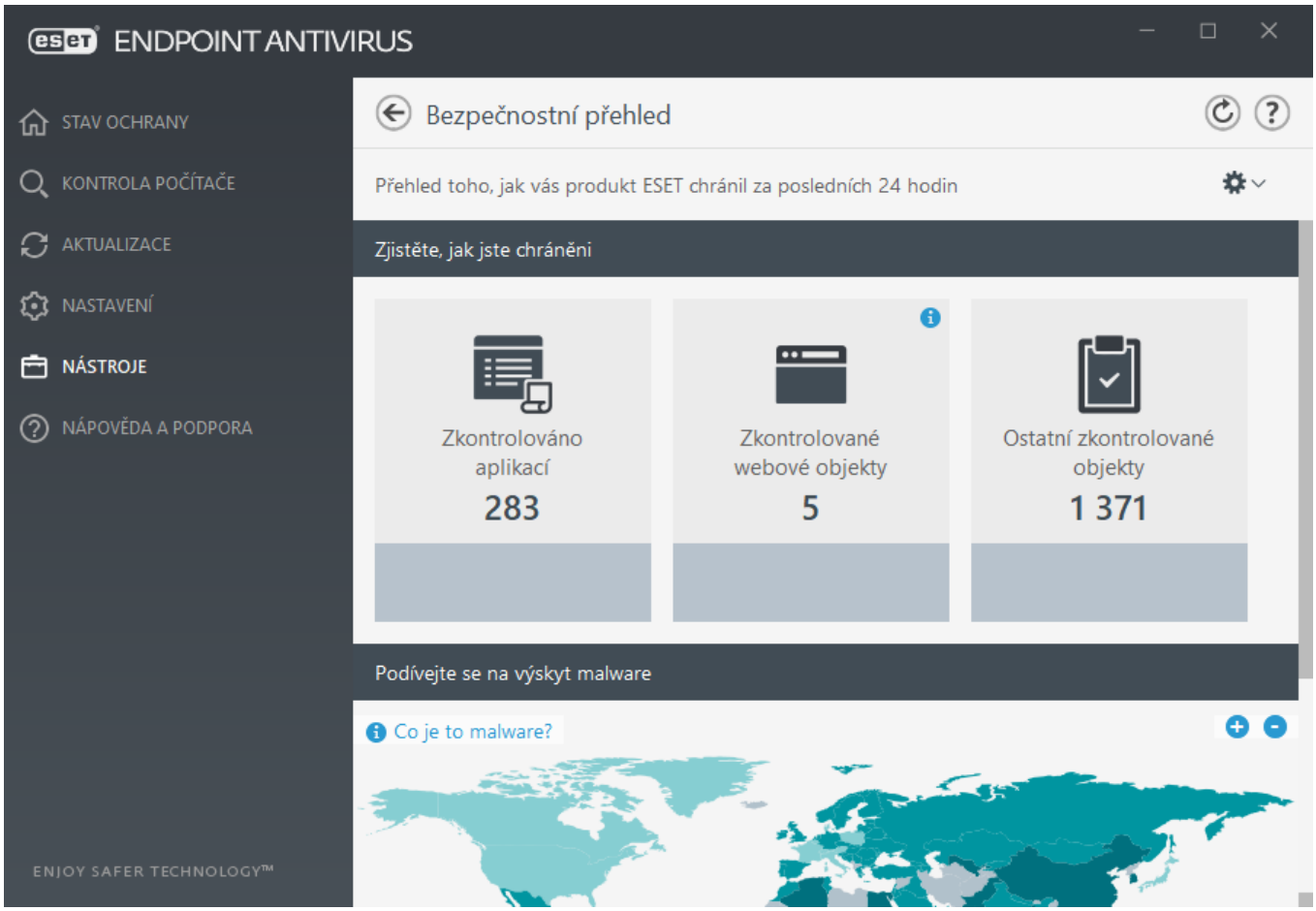
Ostatní zkontrolované objekty – zobrazuje počet dalších zkontrolovaných objektů.

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 ze posledních 30 dní, resp. od aktivace produktu. Pokud jste produkt ESET Endpoint Antivirus 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**.

ESET SysRescue Live

ESET SysRescue Live je bezplatný nástroj, který umožňuje vytvořit bootovatelný záchranný disk (CD/DVD/USB). Následně ze záchranného média můžete nabootovat, provést kontrolu připojených disků a vyléčit infikované soubory.

Hlavní výhodou ESET SysRescue Live je fakt, že běží zcela nezávisle na aktuálně nainstalovaném operačním systému, přičemž má přímý přístup k disku a celému souborovému systému. Díky tomu je takto možné například odstranit infiltraci, kterou nebylo možné vymazat standardním způsobem při spuštěném operačním systému apod.

- Online nápověda pro ESET SysRescue Live

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. Pro nahlášení spamu nebo chybně detekované zprávy jako spam.využijte postup uvedený v Databázi 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 informací o tomto typu útoku naleznete 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) – uveďte URL adresu, případně jeho výrobce (pokud je znám) pro lepší identifikaci.

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

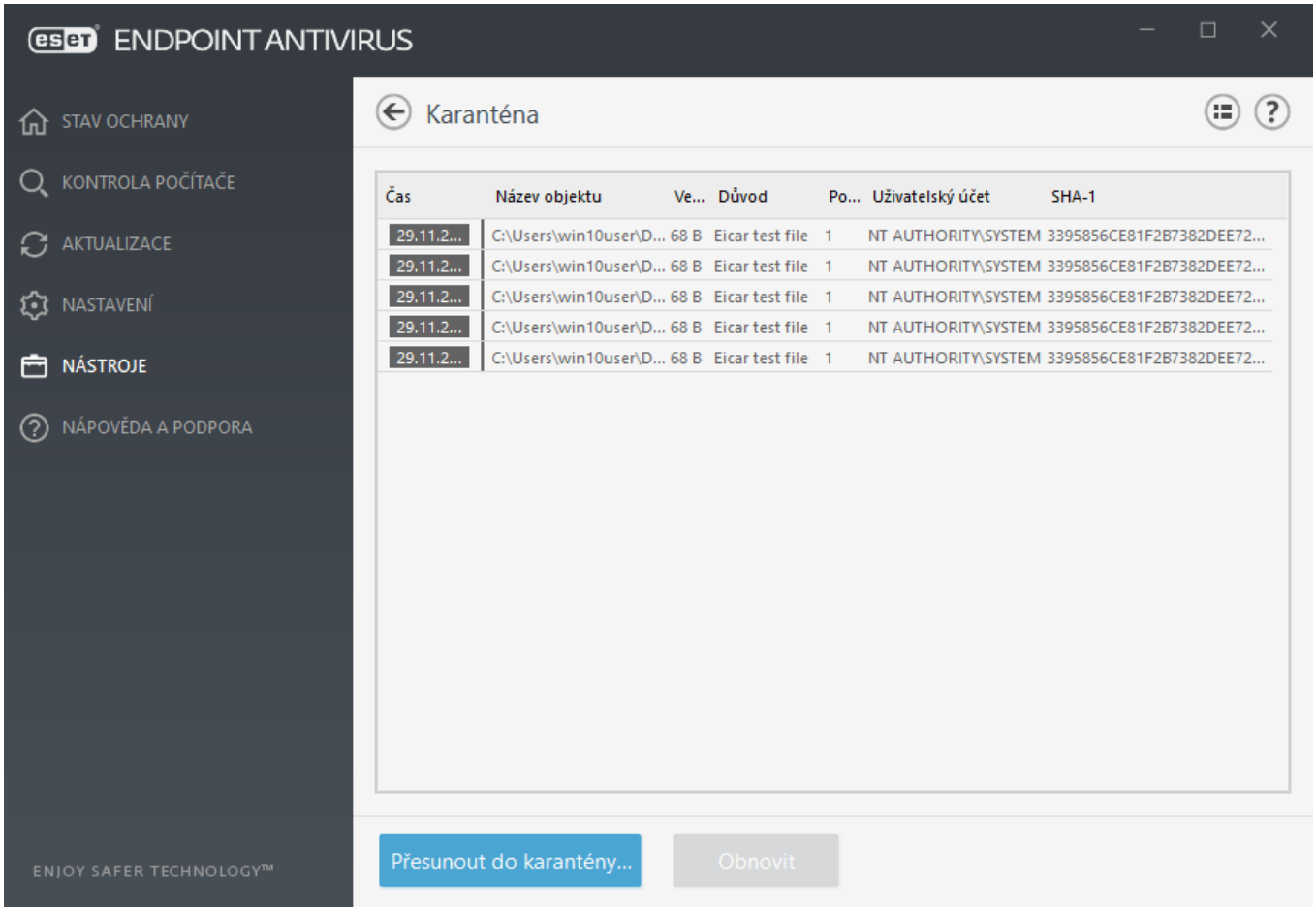
Hlavní funkcí karantény je bezpečně uschovat nahlášené objekty (jako je malware, infikované soubory nebo potenciálně nechtěné aplikace).

Karanténa je dostupná v hlavním okně programu ESET Endpoint Antivirus 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 Antivirus 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:

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

Pro uložení souboru do karantény máte několik možností:

a. 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.
b. Klikněte na **Přidat do karantény** z hlavního okna programu.
c. 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?

Nastavení proxy serveru

Ve velkých lokálních sítích LAN, může připojení do internetu zajišťovat tzv. proxy server. Při použití této konfigurace je třeba definovat následující nastavení. V opačném případě se program nebude moci automaticky aktualizovat. Nastavení proxy serveru je možné definovat v ESET Endpoint Antivirus na dvou odlišných místech v rámci Rozšířeného nastavení.

V prvním případě můžete nastavení serveru konfigurovat v části **Rozšířená nastavení** (F5) > **Nástroje** > **Proxy server**. Tato nastavení specifikují globální nastavení proxy serveru a tyto parametry se použijí pro jakýkoliv modul ESET Endpoint Antivirus. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

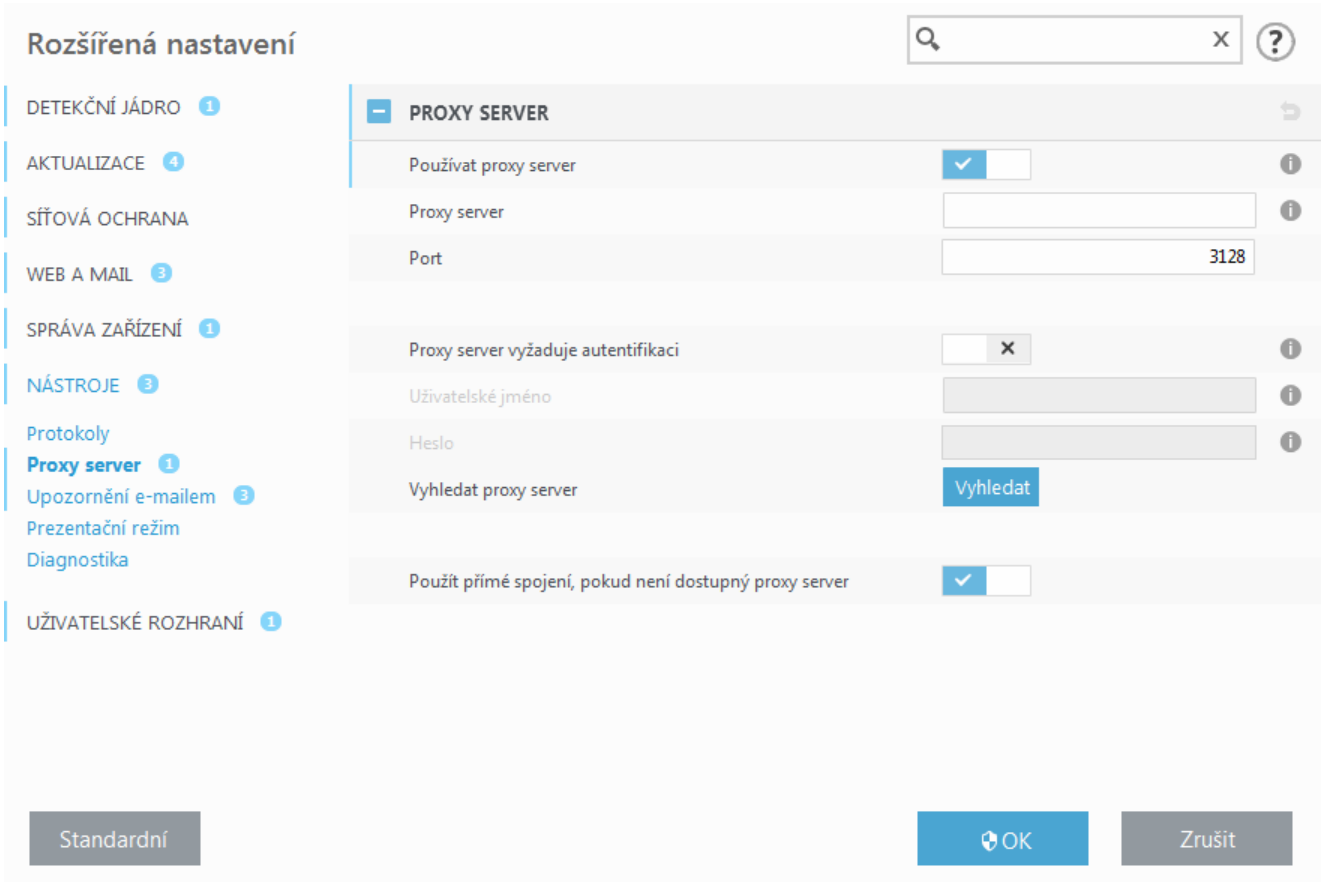
Pro nastavení proxy serveru na této úrovni vyberte možnost **Používat proxy server** a následně zadejte adresu proxy serveru do pole **Proxy server** a číslo portu do pole **Port**.

V případě, že komunikace s proxy serverem vyžaduje autentifikaci, je potřeba také zaškrtnout pole **Proxy server vyžaduje autorizaci** a zadat patřičné údaje do polí **Uživatelské jméno** a **Heslo**. Pro získání automatického nastavení proxy serveru můžete kliknout na tlačítko **Vyhledat**. Tímto se přenese nastavení z operačního systému. Pro zjištění nastavení proxy serveru v operačním systému stiskněte klávesy **Windows + I**, a dále klikněte na **Síť a internet** > **Proxy server**.

Tímto způsobem není možné získat autentifikační údaje (uživatelské jméno a heslo). Pokud jsou pro přístup k **proxy serveru** vyžadovány, musíte je zadat ručně.

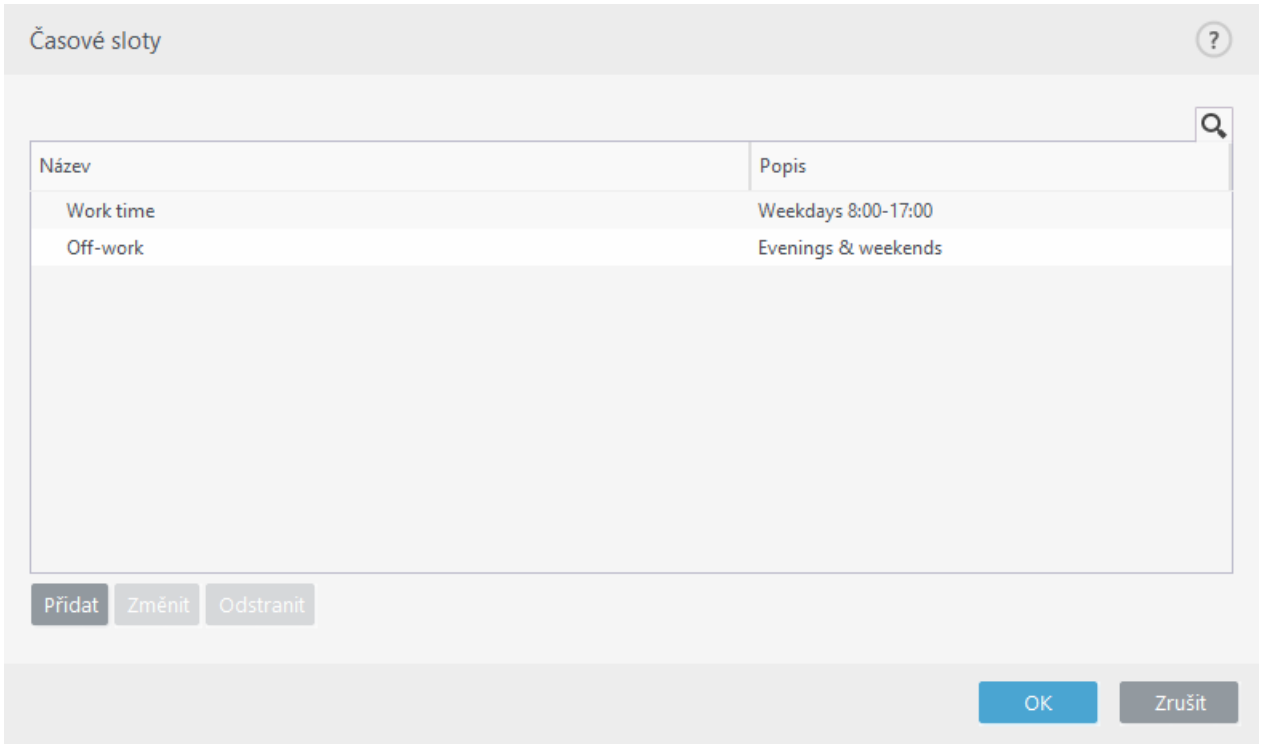
Použít přímé spojení, pokud není dostupný proxy server – pokud máte nastaveno, že se má ESET Endpoint Antivirus připojovat k serverům ESET prostřednictvím proxy, po aktivování této možnosti se produkt pokusí navázat spojení bez použití proxy.

V druhém případě se **nastavení proxy serveru** nachází v **Rozšířeném nastavení** na záložce **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení**). Toto nastavení je platné pro konkrétní profil aktualizace a je vhodné jej použít, pokud se jedná o přenosný počítač, který se aktualizuje z různých míst. Bližší popis nastavení naleznete v kapitole Pokročilé nastavení aktualizace.



Časové sloty

Časové sloty můžete používat při tvorbě pravidel pro **správu zařízení**. 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. Nově vytvořený časový slot můžete následně vybrat pomocí rozbalovacího menu **Aplikovat v době** při vytváření pravidla pro správu zařízení.

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 Antivirus 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.

Interval ověření licence

ESET Endpoint Antivirus se automaticky připojuje k serverů ESET. Pro změnu tohoto chování přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) do sekce **Nástroje** > **Licence**). Ve výchozím nastavení je **Interval ověření** nastaven na **Automaticky**, a produkt komunikuje s licenčními servery ESET několikrát za hodinu. V případě potřeby můžete změnit Interval ověření na **Omezeně**, a snížit tak množství přenášených dat. Mějte na paměti, že produkt se následně k licenčním serverům připojí jednou za den, případně po restartování počítače.

Pokud nastavíte **Interval ověření** na **Omezeně**, všechny změny související s licencí provedené na portále ESET Business Account / ESET MSP Administrator se mohou v produktu ESET Endpoint Antivirus projevit až po uplynutí jednoho dne.

Uživatelské rozhraní

V sekci **Uživatelské rozhraní** můžete konfigurovat nastavení uživatelského rozhraní (GUI).

V části prvky uživatelského rozhraní můžete přizpůsobit vzhled rozhraní a množství použitých efektů.

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu přejděte do sekce Přístup k nastavení a nastavte si heslo.

Nastavením v sekci Upozornění a události a Oznámení změníte chování varování při detekci a chování systémových upozornění. Tato oznámení si můžete nastavit dle svých potřeb.

Pokud se rozhodnete nezobrazovat určitá varování, jejich seznam naleznete v části **Prvky uživatelského rozhraní** > **Stavy aplikací**. Zde můžete zjistit jejich stav a případně znovu povolit jejich zobrazování.

Kontextové menu se zobrazí po kliknutí pravým tlačítkem myši na vybraný objekt. Tento nástroj použijte pro integraci ovládacích prvků ESET Endpoint Antivirus do kontextového menu.

Prezentační režim je vhodný pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru.

Dále se můžete podívat na to, jak minimalizovat uživatelské rozhraní ESET Endpoint Antivirus (užitečné v případě spravovaných prostředí).

Prvky uživatelského rozhraní

Uživatelské rozhraní programu ESET Endpoint Antivirus 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 Antivirus a spusťte aplikaci jako administrátor. Případně můžete režim zobrazení změnit prostřednictvím politiky definované v ESET PROTECT.

Pomocí možnosti **Zobrazit úvodní obrázek při startu** zapnete nebo vypnete zobrazování úvodního obrázku při spouštění ESET Endpoint Antivirus.

Pokud chcete, aby ESET Endpoint Antivirus 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 Antivirus do kontextového menu.

Stavy aplikace

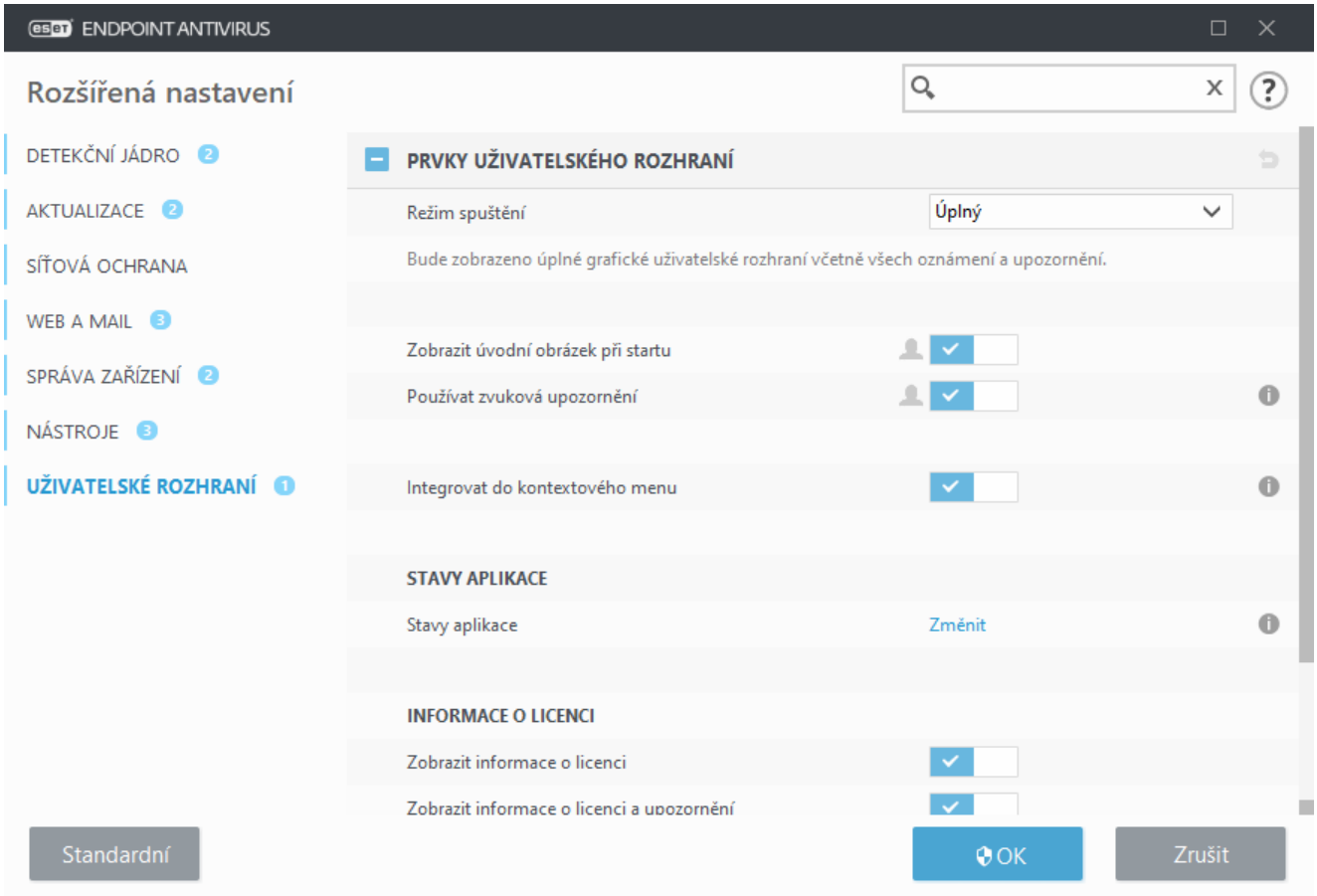
Stavy aplikace – po kliknutí na **Změnit** můžete zapnout nebo vypnout zobrazování stavů aplikace v hlavním okně na záložce **Stav ochrany**.

Informace o licenci

Zobrazit informace o licenci – pokud deaktivujete tuto možnost, na záložce **Stav ochrany** a **Nápověda podpora** se nezobrazí informace o licenci.

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 Antivirus aktivovaném prostřednictvím MSP licence nejsou dostupná.



Přístup k nastavení

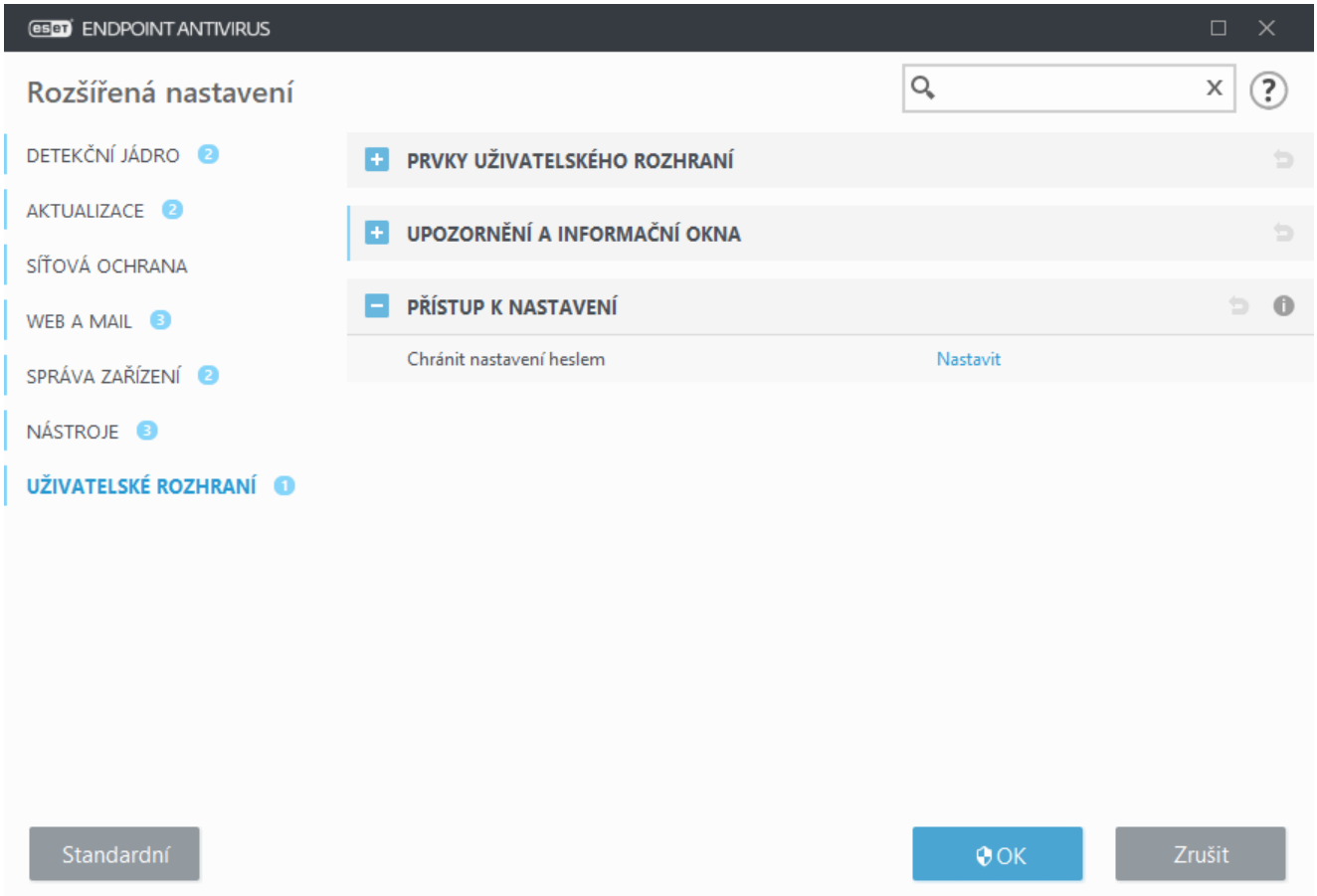
Správné nastavení produktu ESET Endpoint Antivirus je velmi důležité pro zachování celkové bezpečnosti systému. Jeho neoprávněná změna může vést ke snížení zabezpečení systému a ztrátě dat. Pro zabránění neautorizovaných změn v konfiguraci ESET Endpoint Antivirus můžete přístup do rozšířeného nastavení produktu ochránit heslem.

Spravované prostředí

Administrátor může vytvořit politiku, a na spravovaných počítačích hromadně nastavit heslo pro ochranu nastavení produktu ESET Endpoint Antivirus. Pro vytvoření politiky postupuje podle kroků uvedených v kapitoleOchrana produktu heslem.

Nespravované prostředí

Pro ochranu nastavení heslem přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) do sekce **Uživatelské rozhraní** > **Přístup k nastavení**).



Chránit nastavení heslem – zamkne/odemkne nastavení programu. Po kliknutí se zobrazí dialogové okno pro zadání hesla.

Pro nastavení změnu stávajícího hesla klikněte na **Nastavit heslo**.

Heslo pro přístup do Rozšířeného nastavení

Neoprávněným změnám v konfiguraci ESET Endpoint Antivirus zabráníte nastavením hesla, které ochrání nejen konfiguraci, ale znemožní také vypnutí a odinstalaci produktu.

Spravované prostředí

Administrátor může vytvořit politiku, a na spravovaných počítačích hromadně nastavit heslo pro ochranu nastavení produktu ESET Endpoint Antivirus. 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 Antivirus.

Pokud heslo zapomenete, pro obnovení využijte některou z níže uvedených možností.

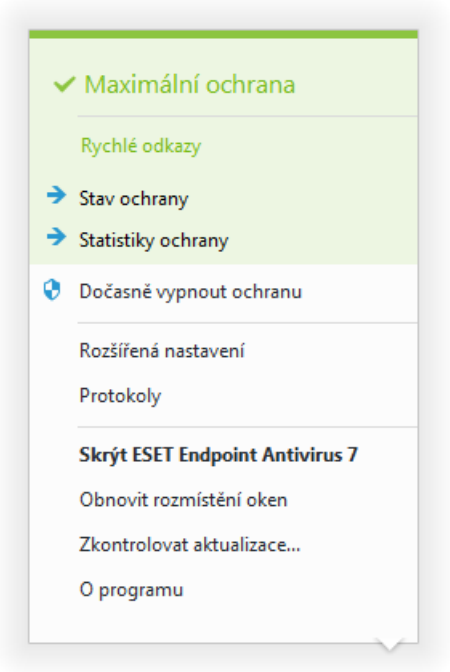
- Obnovení hesla prostřednictvím možnosti "Obnovit heslo" (pro verzi 7.1 a novější)
- Obnovení prostřednictvím nástroje ESET Unlock Tool (verze 7.0 a starší)

Pokud jste ztratili licenční údaje, potřebujete ověřit datum platnosti nebo jakékoli další informace týkající se vaší licence na produkt ESET Endpoint Antivirus, postupujte podle kroků uvedených v Databázi znalostí.

Ikona v oznamovací oblasti

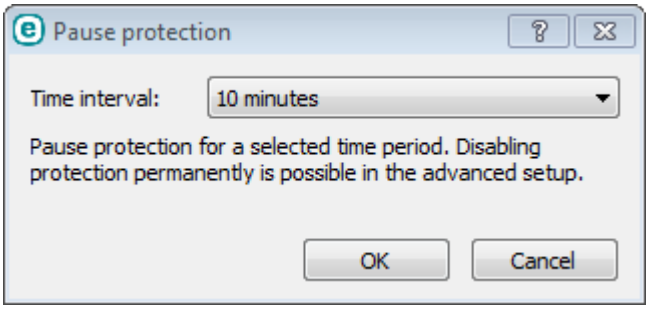
Nejdůležitější možnosti a funkce programu jsou dostupné přímo ze systémové oznamovací oblasti. Stačí kliknout pravým tlačítkem myši na ikonu programu

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 **Časový interval** můžete nastavit dobu, po kterou budou všechny součásti ochrany vypnuty.



Rozšířená nastavení – po kliknutí se zobrazí Rozšířená nastavení programu. Jiný způsob, jak otevřít toto okno je stisknout klávesu **F5** v hlavním okně programu nebo kliknout na **Nastavení** > Rozšířená nastavení.

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

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

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

Zkontrolovat aktualizace – spustí se aktualizace programových modulů pro zajištění maximální ochrany před škodlivým kódem.

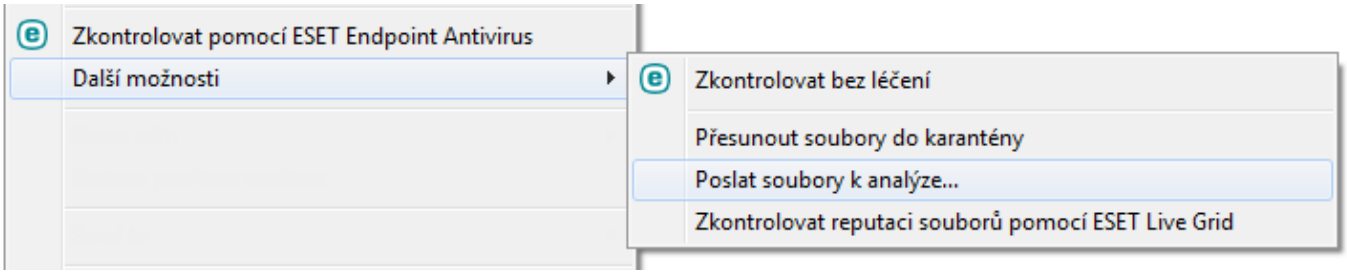
O programu – po kliknutí si zobrazíte informace o systému, nainstalované verzi programu ESET Endpoint Antivirus a všech jeho programovaných modulech. Také zde naleznete datum platnosti licence. Ve spodní části okna se nachází informace o operačním systému a systémových prostředcích.

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 Antivirus. Podrobné nastavení této funkce je dostupné v Rozšířeném nastavení (po stisknutí klávesy F5 v hlavním okně programu) na záložce **Uživatelské rozhraní** > **Kontextové menu**.

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



Nápověda a podpora

ESET Endpoint Antivirus obsahuje informace a nástroje pro řešení problémů včetně možnosti přímo kontaktovat technickou podporu společnosti ESET.

Nainstalovaný produkt

- **O programu ESET Endpoint Antivirus** – kliknutím si zobrazíte souhrnné informace o vámi nainstalovaném programu ESET Endpoint Antivirus.
- **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 Antivirus.

Technická podpora

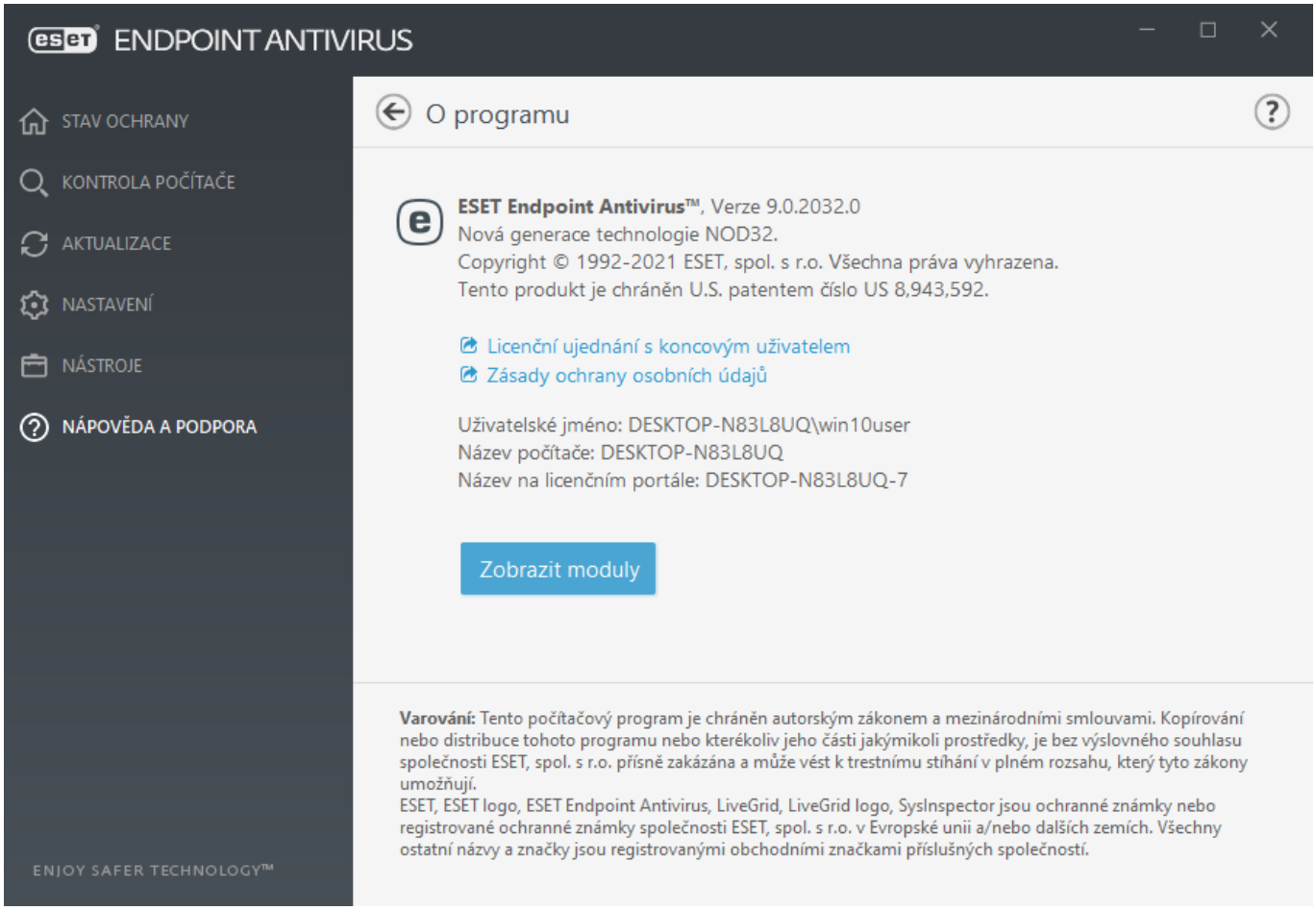
- **Požádat o podporu** – v případě, že nenajdete řešení problému, můžete kontaktovat naše specialisty technické podpory prostřednictvím formuláře na webových stránkách společnosti ESET. V závislosti na konfiguraci produktu se před vyplněním webového formuláře může zobrazit dialogové okno Odeslat konfiguraci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

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 Antivirus

V tomto okně naleznete informace o programu ESET Endpoint Antivirus, informace o operačním systému, systémových prostředcích.

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.



Odeslat konfiguraci systému

Aby mohli specialisté technické podpory rychle a relevantně reagovat na dotazy zákazníků, vyžadují zaslání konfigurace produktu ESET Endpoint Antivirus, detailních informací o systému včetně spuštěných procesů a záznamů v registru – tedy protokolu z nástroje ESET SysInspector. Společnost ESET tato data využívá výhradně při řešení technických problémů s produkty ESET.

Pokud nechcete odeslat žádná data, vyberte možnost Neodesílat data. Mějte na paměti, že specialisté technické podpory vás v tomto případě mohou následně požádat o dodatečné zaslání těchto dat. Chcete-li naopak odesílat data vždy, a nechcete aby se vás program dotazoval, vyberte možnost **Vždy odesílat tato data**.

Možnosti odesílání dat naleznete v **Rozšířeném nastavení** v sekci **Nástroje** > **Diagnostika** > **Technická podpora**.

Pokud se rozhodnete odeslat konfiguraci systému, je nutné vyplnit a odeslat webový formulář se žádostí o technickou podporu. V opačném případě nedojde k vytvoření žádosti a data budou ztracena.

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 přesměrování na stránku 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.

Oznámení

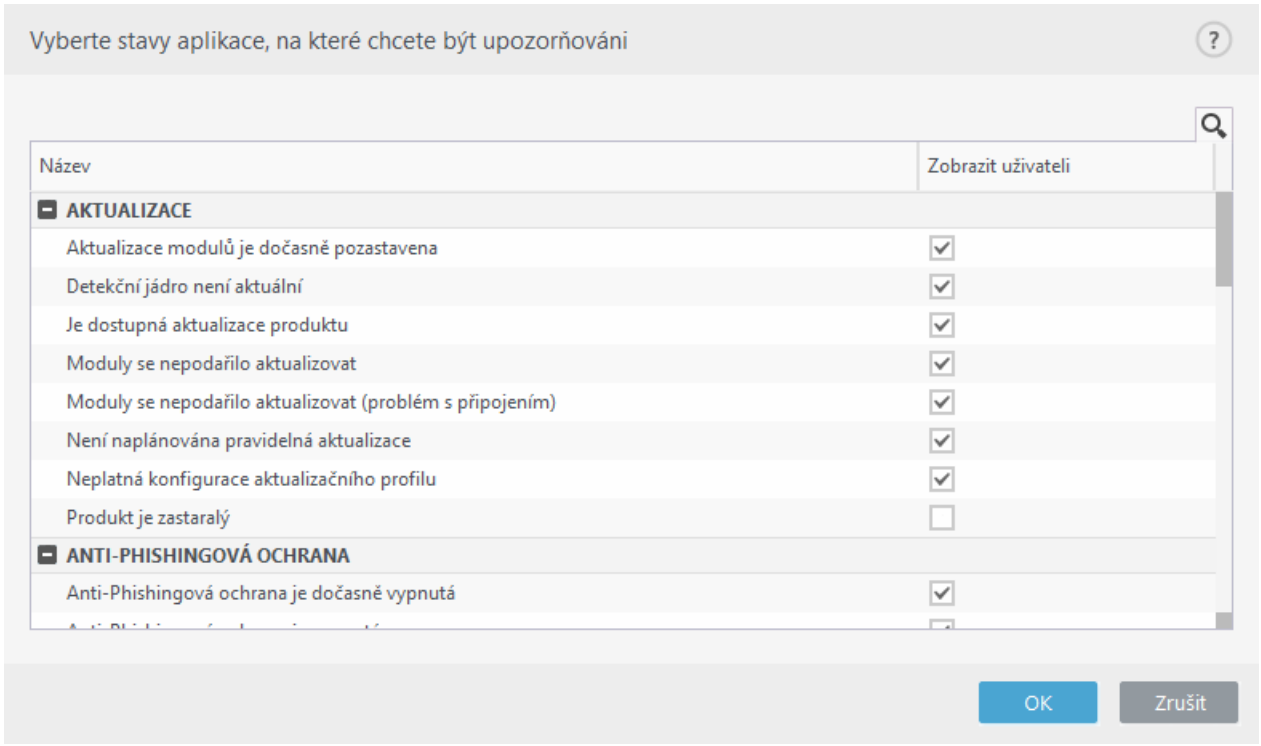
Způsob, jakým bude produkt ESET Endpoint Antivirus komunikovat s uživatelem, můžete definovat v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **Oznámení**. V této části můžete konfigurovat následující typy oznámení:

- Stavy aplikace – po kliknutí na Změnit se můžete rozhodnout, jaké stavy aplikace chcete zobrazovat v **hlavním okně programu**.
- Oznámení na pracovní ploše a bublinové tipy – oznámení zobrazující se jako malá okna nad systémovou oblastí.
- Přizpůsobení oznámení – do oznámení zobrazovaných na ploše si můžete přidat vlastní zprávu.
- Interaktivní upozornění – výstražná upozornění a informační okna, která vyžadují interakci uživatele.
- Přeposílání (e-mailová oznámení) – oznámení se zasílají e-mailem na konkrétní adresy.

Stavy aplikace

Pro přizpůsobení zobrazovaných stavů v hlavním okně programu (například upozornění na dočasně vypnutou antivirovou a antispywarovou ochranu nebo aktivní Herní režim) přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5) do sekce **Oznámení** a na řádku **Stavy aplikace** klikněte na **Změnit**.

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 pop-up okna zobrazovaná v systémové oblasti. Ve výchozím nastavení se zobrazí po dobu 10 sekund a následně pomalu zmizí. Prostřednictvím nich ESET Endpoint Antivirus 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** – e-mailem se odešlou upozornění na chyby a varovné zprávy (například Anti-stealth není funkční nebo selhala aktualizace modulů,
- **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.

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** (F5) a přejděte do sekce **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**.

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.

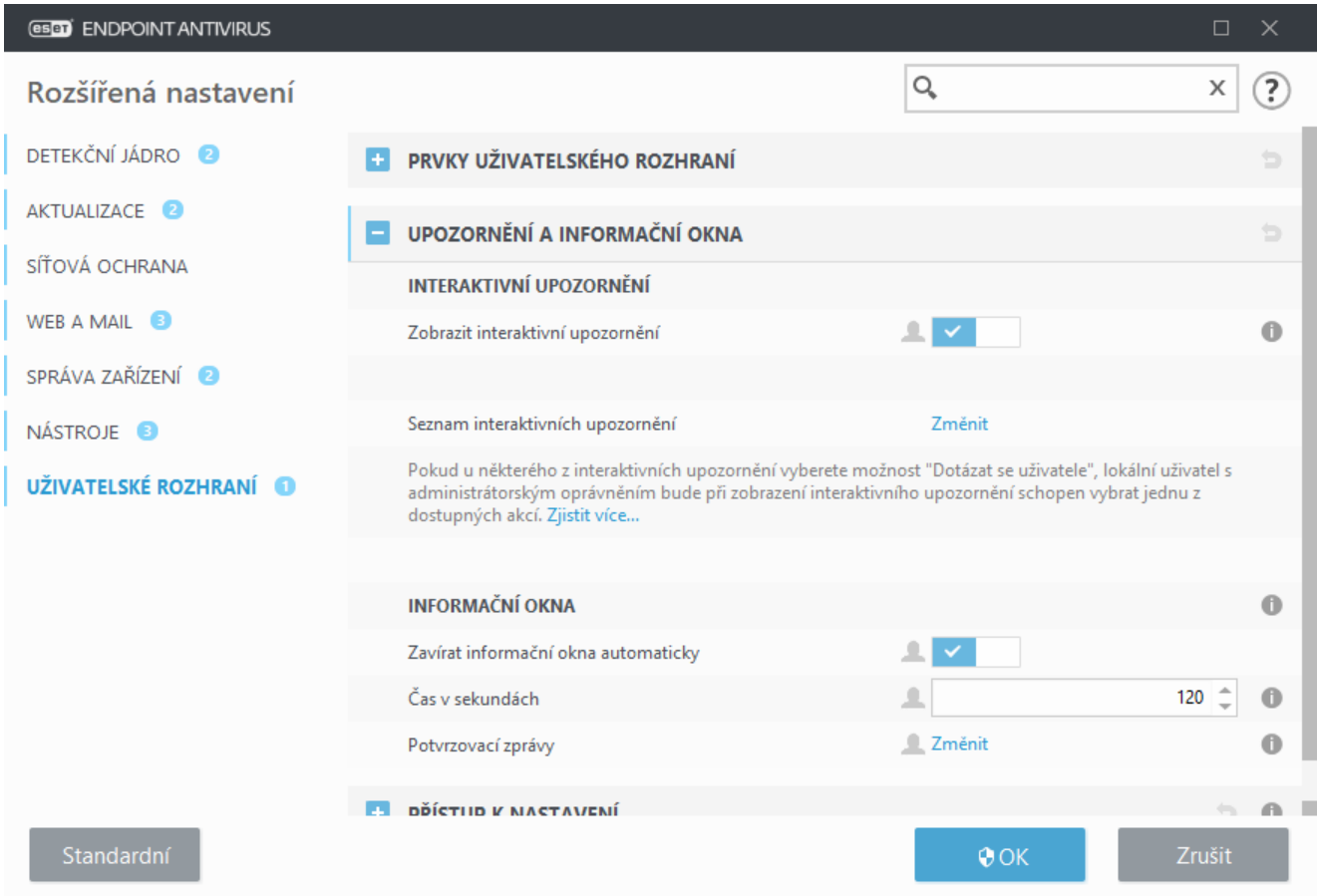
Pokud chcete uživateli zobrazit vlastní zprávu, deaktivujte možnost **Použít výchozí oznámení** a do pole **Zpráva při výskytu detekce** zadejte vlastní text zprávy.

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 sekci **Oznámení** > **Interaktivní upozornění** můžete nastavit, jak se má ESET Endpoint Antivirus zachovat, pokud bude při detekci vyžadovat interakci uživatele (například při pokusu o přístup na potenciálně phishingovou stránku).



Interaktivní upozornění

Interaktivní upozornění se zobrazují v případě výskytu detekce nebo jiné události vyžadující odezvu uživatele.

Zobrazit interaktivní upozornění

- 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.

Deaktivováním možnosti **Zobrazit interaktivní upozornění** se potlačí zobrazování všech výstražných oken a zpráv v internetových prohlížečích. Produkt automaticky provedete předdefinovanou výchozí akci (například zablokuje přístup na potenciálně phishingovou stránku).

Informační okna

Dobu zobrazení informačních upozornění nastavíte pomocí možnosti **Zavírat informační okna automaticky**. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

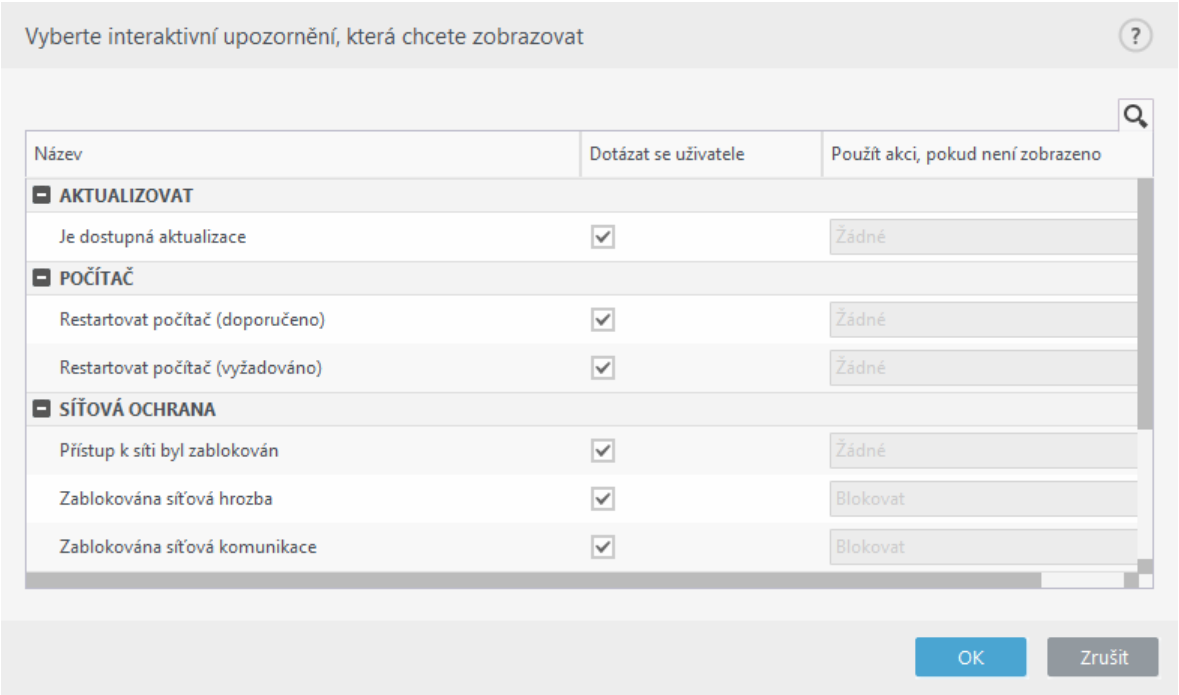
Potvrzovací zprávy – Pomocí této možnosti můžete spravovat seznam potvrzovacích zpráv, jejichž zobrazování chcete povolit nebo zakázat.

Seznam interaktivních upozornění

V této sekci naleznete seznam upozornění, které může produkt ESET Endpoint Antivirus uživateli zobrazit, pokud bude vyžadovat jeho interakci.

Pro změnu chování interaktivních upozornění přejděte v Rozšířeném nastavení produktu ESET Endpoint Antivirus do sekce **Oznámení** > **Interaktivní oznámení** a klikněte na **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.
> Dále se podívejte rovněž na stavy aplikace, jejichž zobrazování můžete potlačit.



Pro vysvětlení jednotlivých interaktivních upozornění se podívejte do relevantních kapitol v této příručce:

Výměnná média

- Rozpoznáno nové zařízení

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

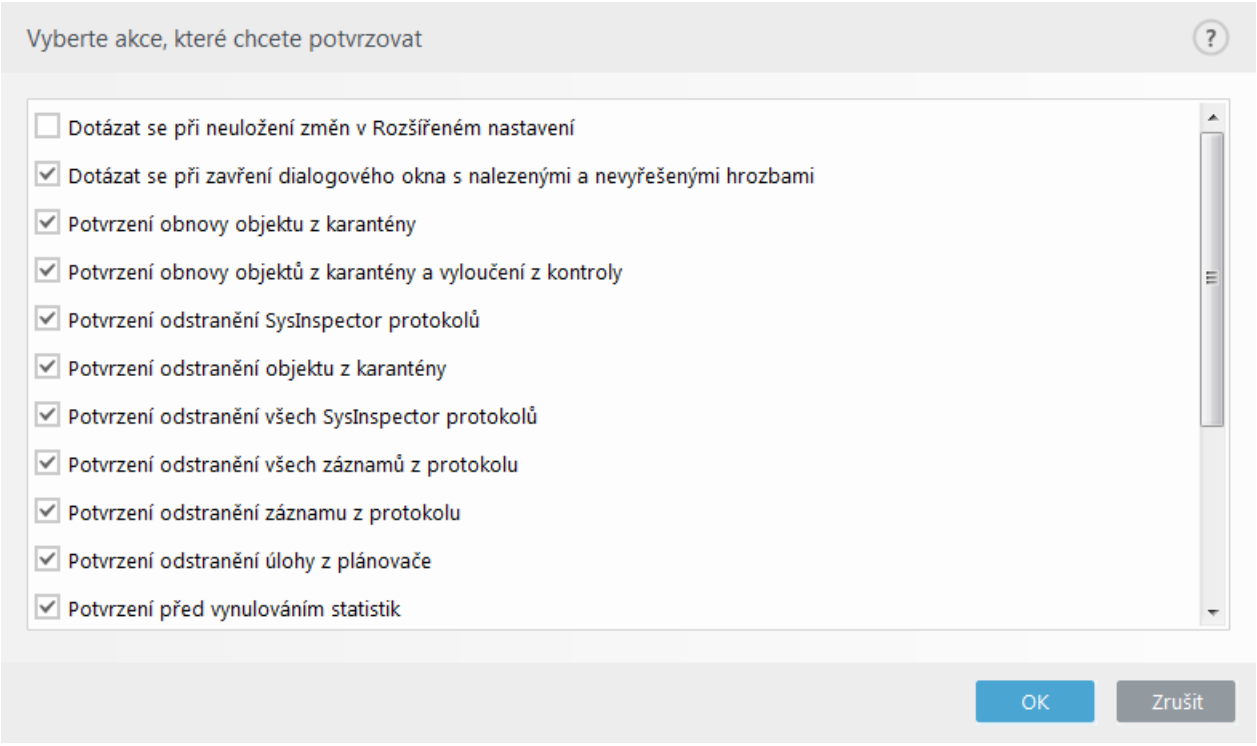
Po zobrazení níže uvedených upozornění se uživatelské rozhraní podbarví oranžově:

- 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 zobrazovaných produktem ESET Endpoint Antivirus přejděte v Rozšířeném nastavení do sekce **Uživatelské rozhraní** > **Upozornění a informační okna** a na řádku **Potvrzovací zprávy** klikněte na **Změnit**.



V tomto dialogovém okně můžete upravit zobrazování zpráv, které ESET Endpoint Antivirus 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 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

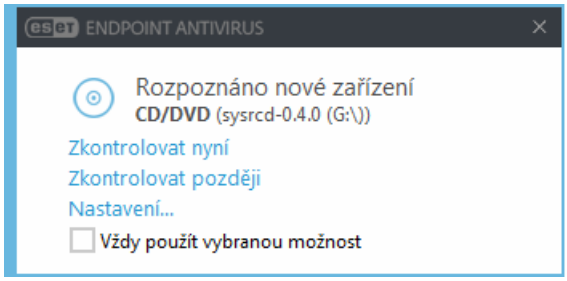
Tato chyba se může zobrazit v případě, kdy máte některou z komponentu (například HIPS) přepnutý do interaktivního nebo učícího režimu, a pokoušíte se vytvořit pravidlo ve stejnou chvíli, jako program.

Před vytvořením vlastním pravidel přepněte režim filtrování na **automatický**. Pro více informací přejděte do kapitoly HIPS a režim filtrování.

Výměnná média

ESET Endpoint Antivirus dokáže automaticky kontrolovat výměnná média (CD/DVD/USB/...) po jejich vložení/připojení do počítače. Tuto funkci můžete využít pro zvýšení zabezpečení, kdy chcete zabránit uživatelům v připojování médií s infikovaným obsahem.

Když připojíte výměnné médium, a v ESET Endpoint Antivirus je nastaveno **Zobrazit možnosti kontroly**, zobrazí se dialogové okno s nabídkou následujících akcí:



Možnosti tohoto dialogu:

- **Zkontrolovat nyní** – spustí se ruční kontrola výměnného média.
- **Nekontrolovat** – neprovede se žádná akce.

Kromě toho modul Správa zařízení ESET Endpoint Antivirus disponuje pokročilými funkcemi, které vám umožňují

definovat pravidla pro zacházení s externími zařízeními připojovanými k vašemu počítači. Více informací naleznete v kapitole Správa zařízení.

Pro konfiguraci kontroly výměnných médií si otevřete Rozšířená nastavení (**F5**) a přejděte do sekce **Uživatelské rozhraní** > **Upozornění a informační okna** > **Interaktivní upozornění** a klikněte na **Změnit** na řádku **Seznam interaktivních upozornění**. Následně nastavte položku **Detekováno nové zařízení**.

Pokud není aktivní možnost **Dotázat se uživatele**, vyberte akci, která se provede automaticky po připojení výměnného média k počítači:

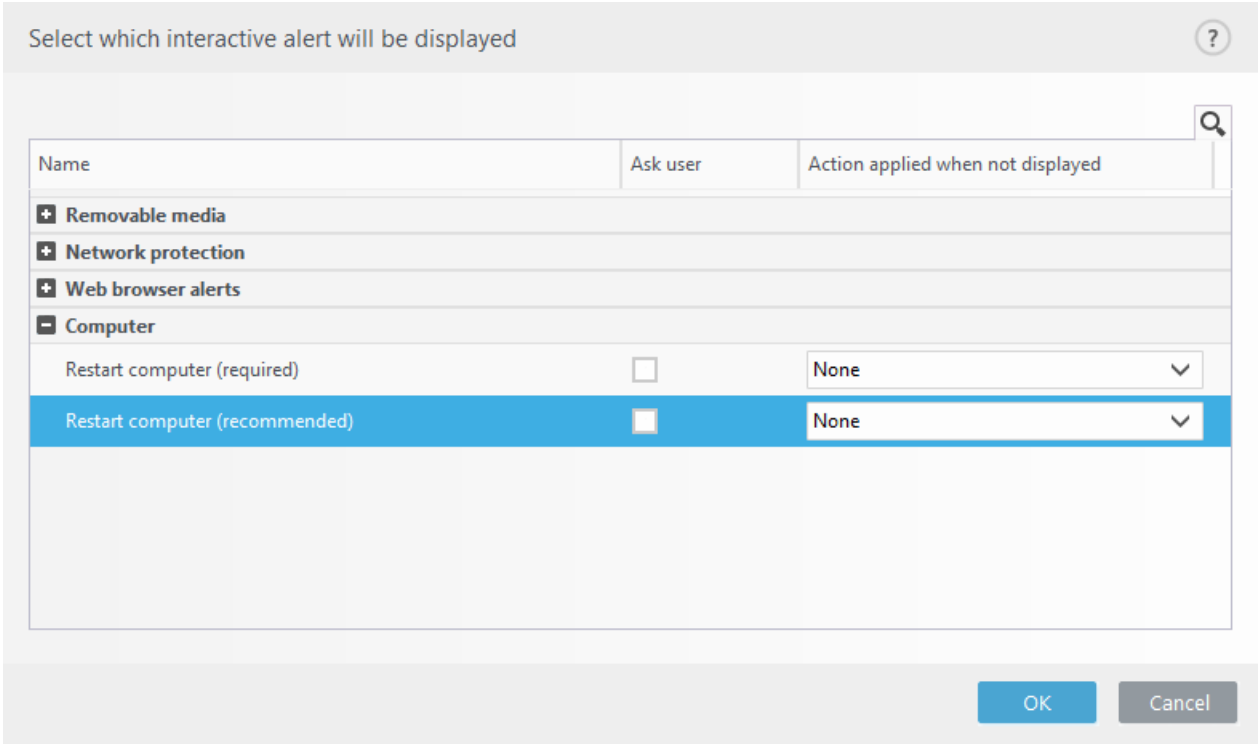
- **Nekontrolovat** – neprovede se žádná akce a upozornění **Nalezeno nové nařízení** se nezobrazí.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí kontrola jeho obsahu.
- **Vynucená kontrola zařízení** – po vložení média se automaticky spustí kontrola jeho obsahu, kterou nelze přerušit.
- **Zobrazit možnosti kontroly** – po kliknutí se přesunete v nastavení do sekce **Interaktivní upozornění**.

Vyžadován restart

Pokud klient začne zobrazovat informaci "Vyžadován restart", uživatelské rozhraní se podbarví červeně. V případě potřeby můžete zobrazování tohoto upozornění oznámení potlačit.

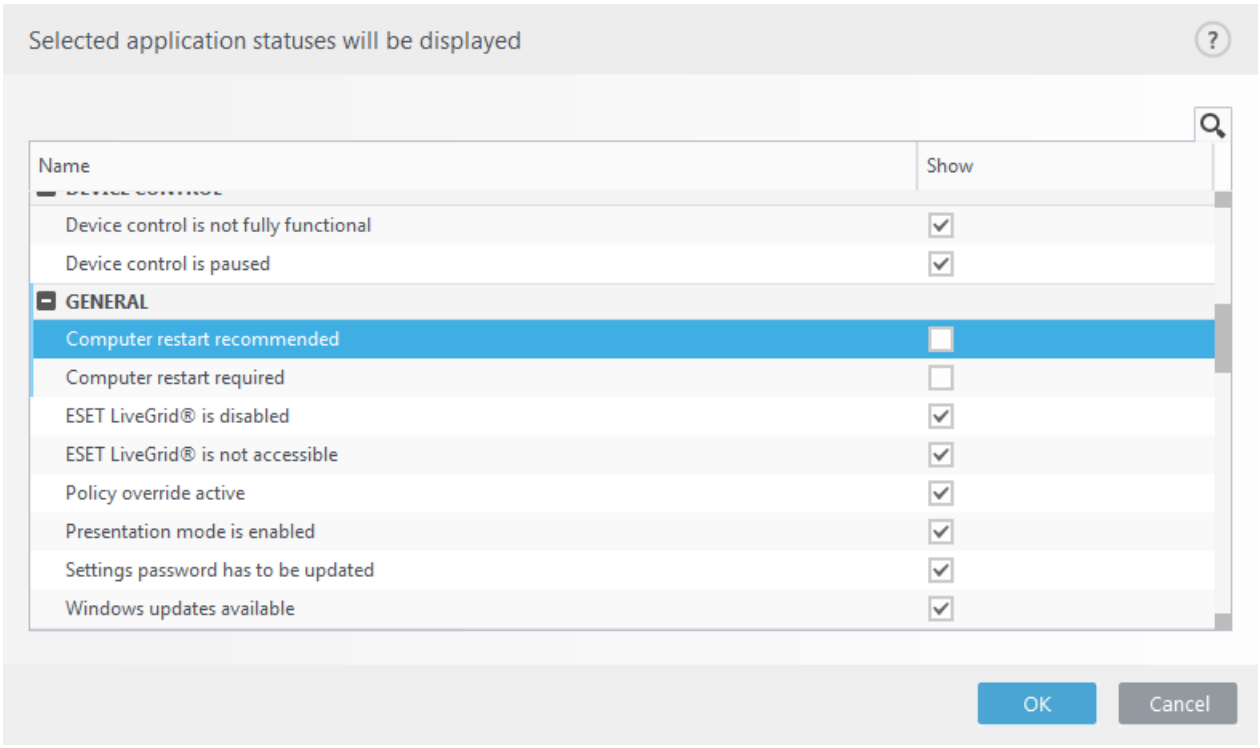
Pro deaktivování zobrazování upozornění "Doporučen restart" a "Vyžadován restart" postupujte podle níže uvedených kroků:

1. V hlavním okně programu stiskněte klávesu **F5** a v Rozšířeném nastavení přejděte do sekce **Uživatelské rozhraní** > **Upozornění a informační okna**.
2. Na řádku **Seznam interaktivních 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 Antivirus.

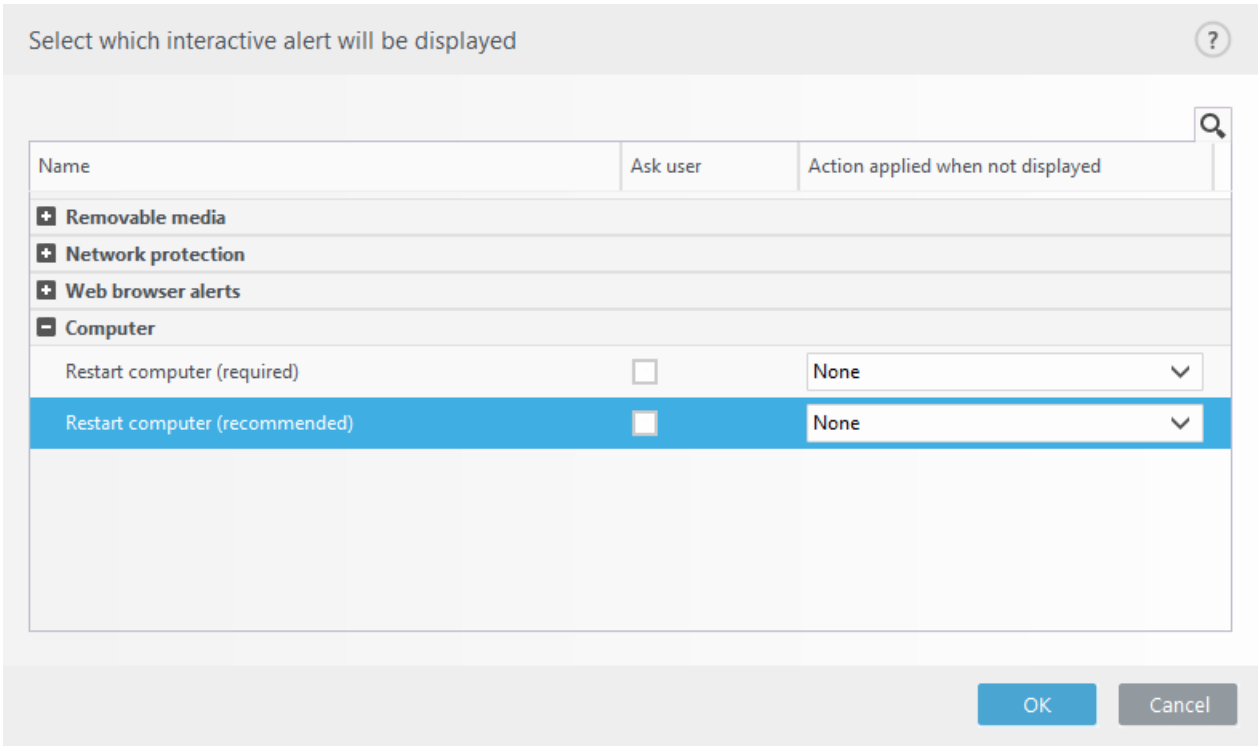


Doporučen restart

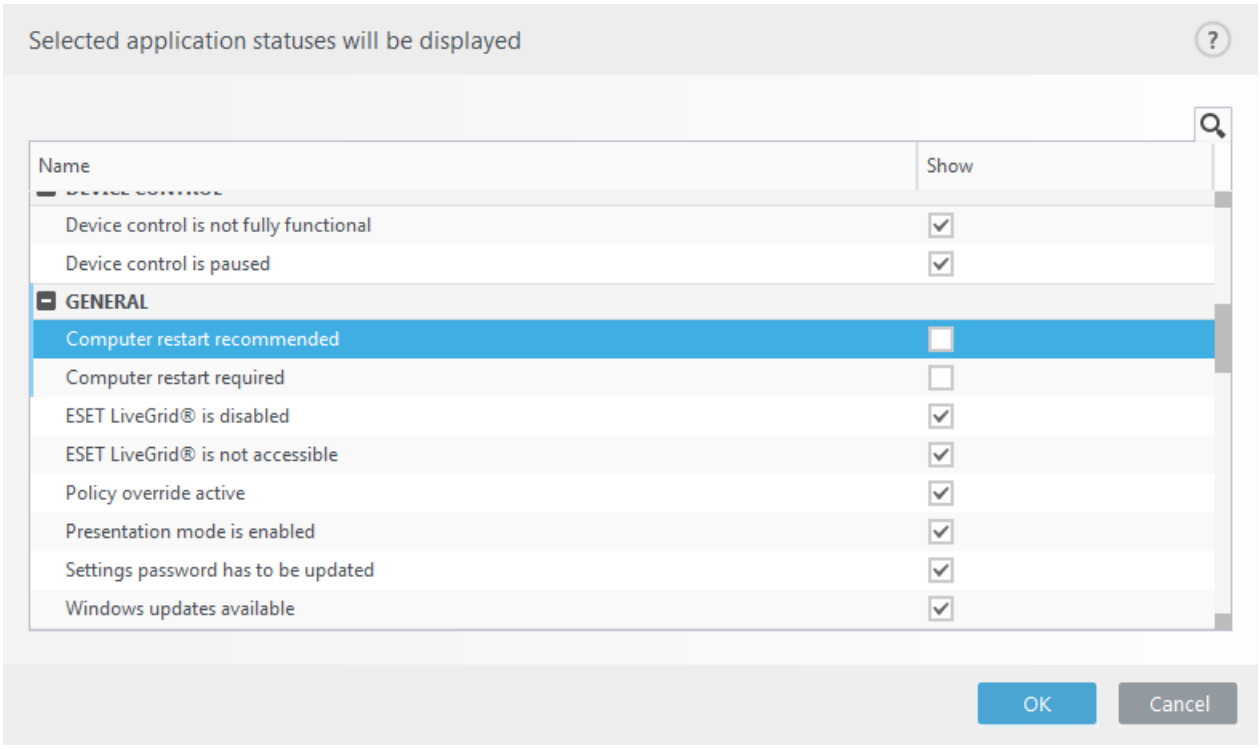
Pokud klient začne zobrazovat informaci "Doporučen restart", uživatelské rozhraní se podbarví žlutě. V případě potřeby můžete zobrazování tohoto upozornění oznámení potlačit.

Pro deaktivování zobrazování upozornění "Doporučen restart" a "Vyžadován restart" postupujte podle níže uvedených kroků:

1. V hlavním okně programu stiskněte klávesu **F5** a v Rozšířeném nastavení přejděte do sekce **Uživatelské rozhraní** > **Upozornění a informační okna**.
2. Na řádku **Seznam interaktivních 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 Antivirus.

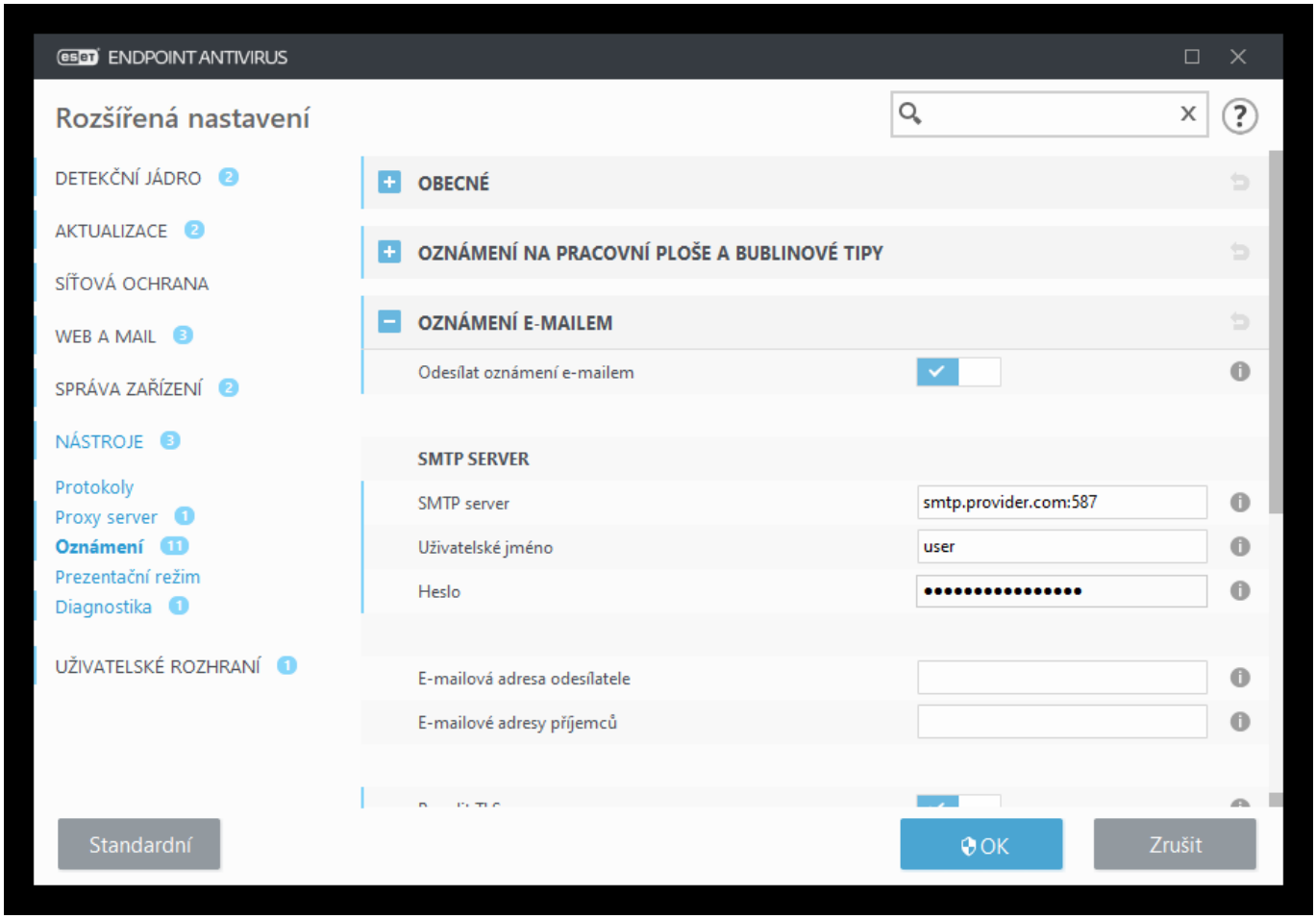


Přeposílání

ESET Endpoint Antivirus dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pro aktivování zaslání upozornění e-mailem přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) do sekce **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.



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 Antivirus 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.

Nastavení e-mailu

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** – e-mailem se odešlou upozornění na chyby a varovné zprávy (například Anti-stealth není funkční nebo selhala aktualizace modulů,
- **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).

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.

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.

Správa profilů

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

Volitelné kontroly 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 **Rozšířené nastavení** (dostupné po stisknutí klávesy F5 v hlavním okně programu), přejděte na záložku **Antivir** > **Volitelná kontrola počítače**. Kliknutím na **Změnit** na řádku **Profily** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. V kapitole parametry skenovacího jádra ThreatSense naleznete popis jednotlivých parametrů pro nastavení kontroly počítače.

> Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy nebo potenciálně nebezpečné aplikace a přitom požadujete **Přísné léčení**? 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 umožňuje vytvořit 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.

Klávesové zkratky

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

Klávesové zkratky	Akce
F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Up/Down	umožní pohyb mezi položkami v produktu
TAB	přesune se na další položku v rámci okna
Esc	zavře aktivní dialogové okno
Ctrl+U	zobrazí dialogové okno se základními informacemi pro technickou podporu ESET, kde mj. najdete identifikátor své licence
Ctrl+R	obnoví pozici a velikost okna na výchozí hodnoty

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 Antivirus.

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 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 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. Tato možnost je dostupná od verze 7.2.

Aktivovat rozšířené protokolování licence – po aktivování této možnosti se zaznamená veškerá komunikace produktu s licenčními servery (ESET Business Account).

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 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 diagnostické protokolování filtrování protokolů – do souboru v PCAP formátu bude zaznamenána veškerá síťová komunikace probíhající po kontrolovaných protokolech. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem filtrování protokolů.

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 – po aktivování této možnosti se zaznamenají všechny akce související s fungováním rezidentní ochrany souborového systému. Toto pomůže vývojářům při diagnostice a řešení problémů.

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.

Umístění protokolů

C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics

Skener příkazového řádku

Modul antivirové ochrany produktu ESET Endpoint Antivirus 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.

ESET CMD

Jedná se o funkci, která povolí používání pokročilých ecmd příkazů. Díky tomu můžete exportovat a importovat nastavení prostřednictvím příkazového řádku (ecmd.exe). Až dosud bylo možné exportovat nastavení pomocí GUI. Export konfigurace ESET Endpoint Antivirus 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, nebudete vyžadována autentifikace. 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. 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 Antivirus 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:

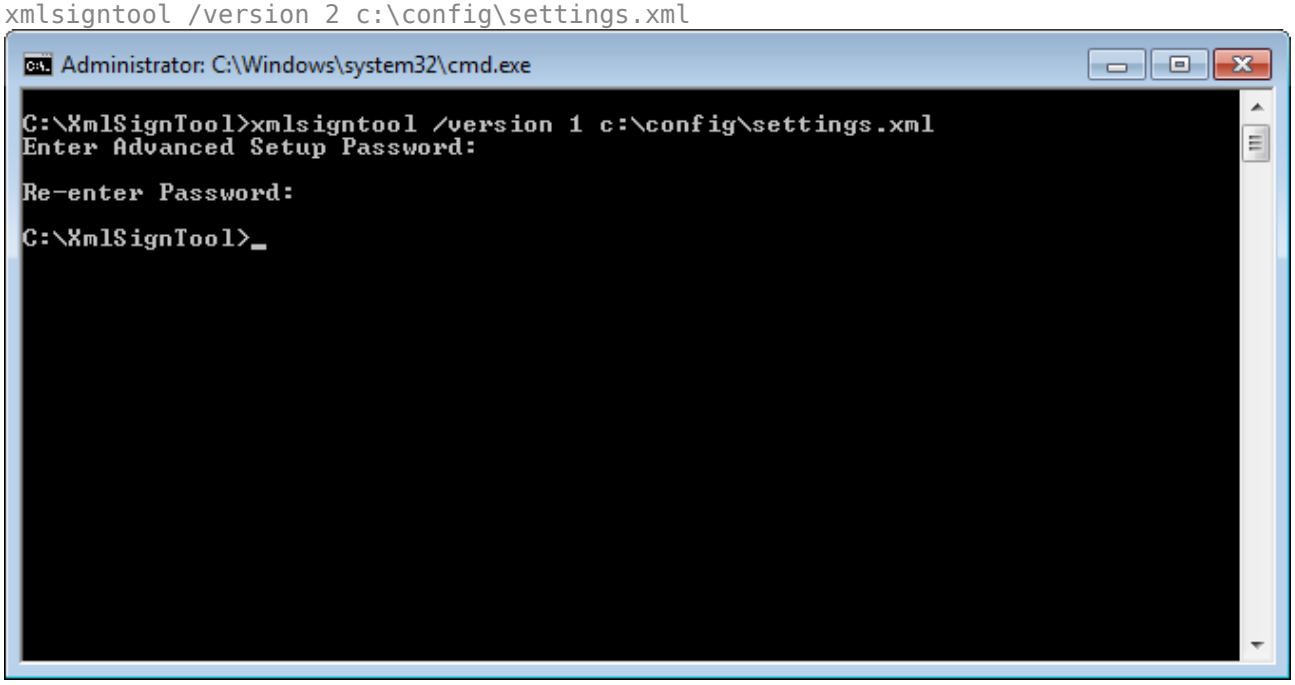
1. Z webových stránek společnosti ESET si stáhněte nástroj XmlSignTool. Jedná se o oficiální nástroj určený pro podepisování konfiguračních souborů.
2. Příkazový řádek **Spusťte jako administrátor** (cmd).
3. Přejděte do složky se staženým nástrojem `xmlsigntool.exe`.
4. Konfigurační příkaz *.xml* podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`

Hodnota parametru `/version` závisí na verzi ESET Endpoint Antivirus. 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 Antivirus.

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. V opačném případě byste museli konfiguraci znovu exportovat z jiné instalace ESET Endpoint Antivirus.

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
Anti-Stealth ochrana	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable

Bezpečnostní funkce	Příkaz pro dočasné pozastavení	Příkaz pro zapnutí
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	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-Phishingová ochrana	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Detekce stavu nečinnosti

Nastavení Detekce stavu nečinnosti můžete konfigurovat v části **Rozšířené nastavení** > **Detekční jádro** > **Detekce škodlivého kódu** > **Kontrola při nečinnosti** > **Detekce stavu nečinnosti**. Produkt dokáže detekovat následující stavy, které využívá jako podnět pro spuštěníkontroly při nečinnosti:

- aktivní spořič obrazovky,
- uzamčení počítače,
- odhlášení uživatele.

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

Import a export nastavení

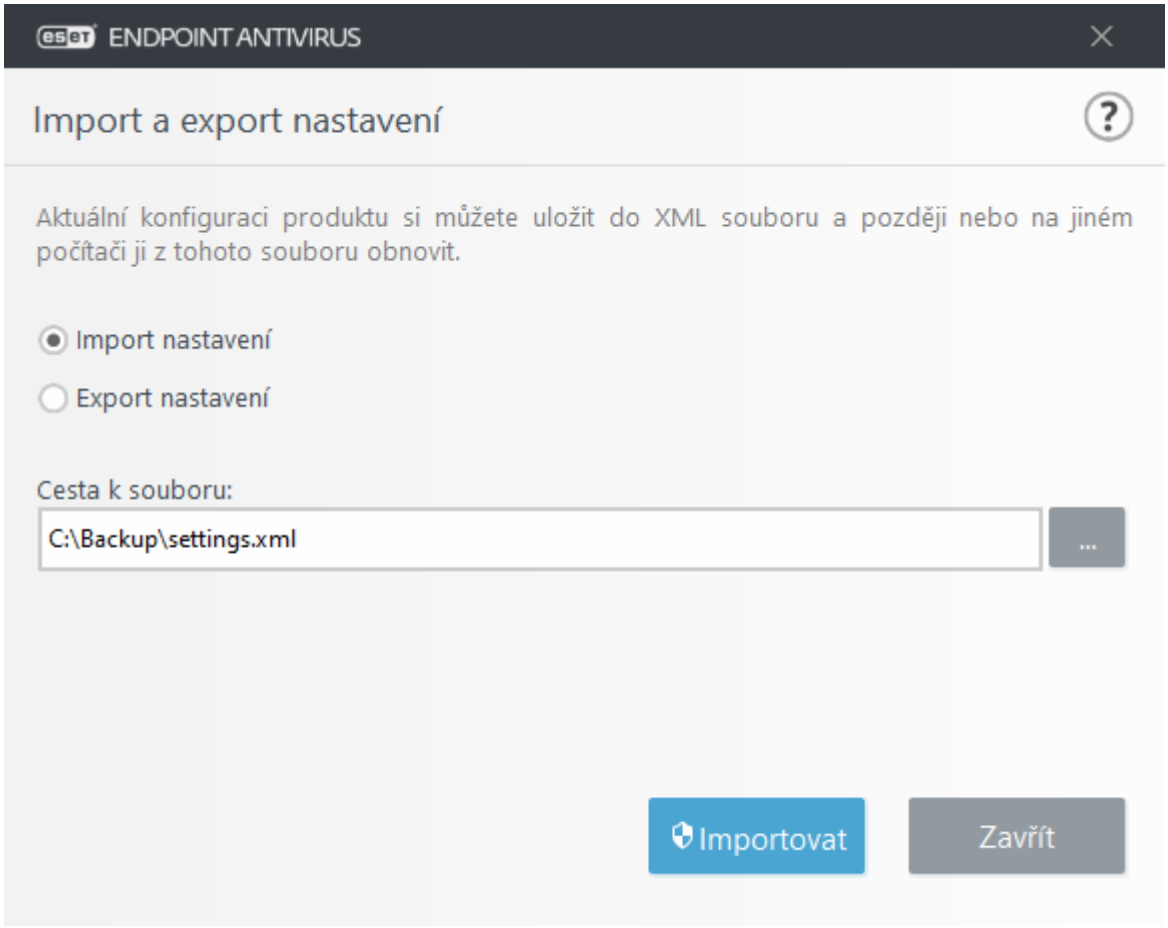
Na záložce **Nastavení** můžete do programu ESET Endpoint Antivirus importovat nebo z něj naopak exportovat konfiguraci v .xml souboru.

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

Import nastavení je velmi jednoduchý. 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.

Kroky pro export konfigurace jsou velmi podobné. 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 (například *C:\export.xml*). 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.



Obnovit všechna nastavení na standardní

Pro obnovení veškerých nastavení produktu včetně jednotlivých modulů na výchozí hodnoty klikněte v rozšířeném nastavení (dostupném po stisknutí klávesy F5 v hlavním okně programu) na tlačítko **Standardní**. 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.

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 Antivirus 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 Antivirus?

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

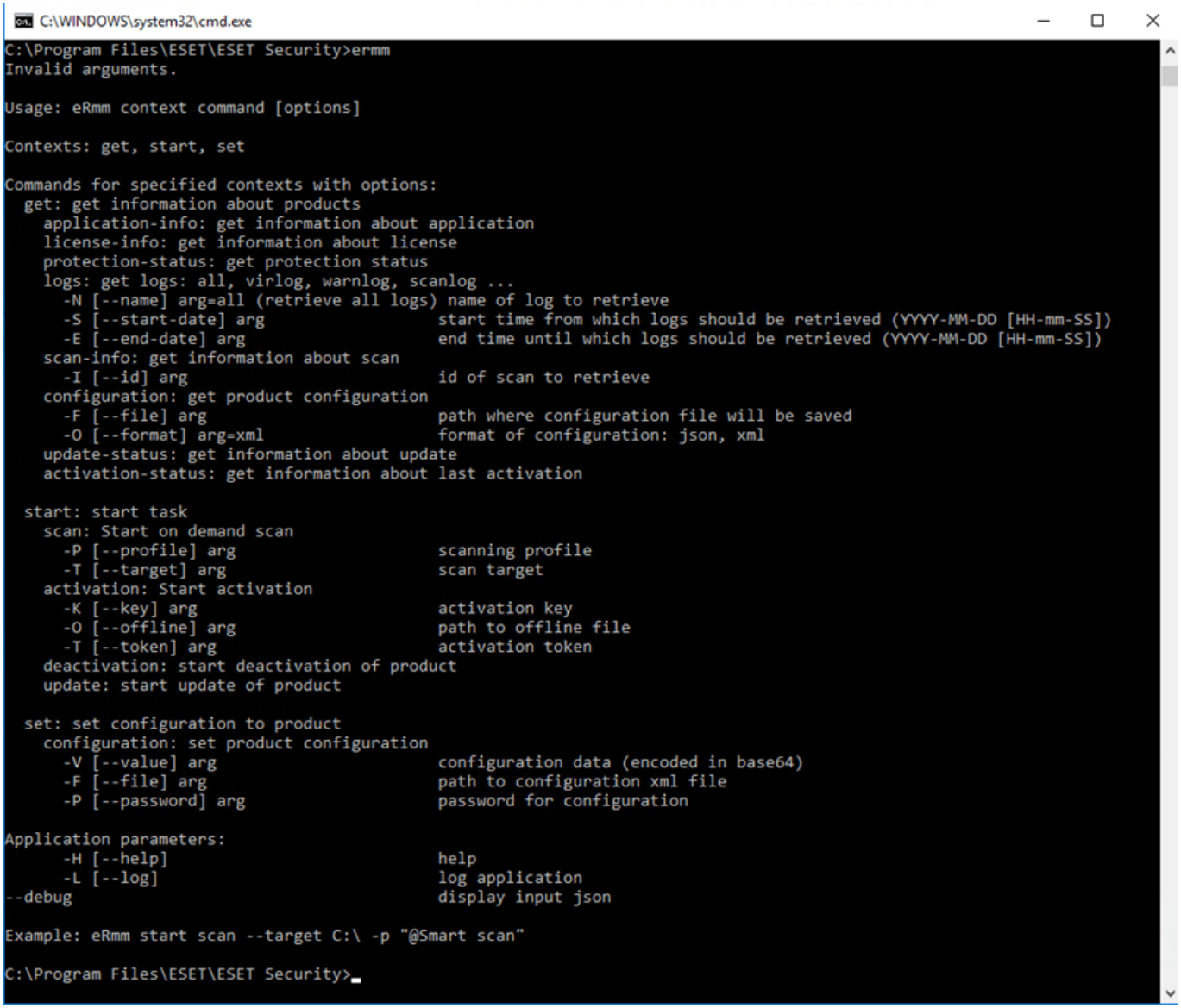
ERMM příkazový řádek

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start		**Start task**
	scan	Start on demand scan
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		**Set options for product**
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

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

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

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

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

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":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"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

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

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

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

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])

Example

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 }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

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 }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

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 }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

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

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

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

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

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

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

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

Command line

```
ermm.exe start update
```

Parameters

None

Example

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 }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

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)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

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 Antivirus?
- Jak aktivovat ESET Endpoint Antivirus?
- Jak použít uživatelské jméno a heslo pro aktivaci produktu?
- Jak odstranit vir z počítače?
- 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 Antivirus
- Jak vytvořit mirror?
- Jak přejít na Windows 10 s nainstalovaným ESET Endpoint Antivirus?
- Jak aktivovat vzdálené monitorování a správu produktu (RMM)?
- Jak zablokovat stahování konkrétních typů souborů?
- Jak minimalizovat uživatelské rozhraní ESET Endpoint Antivirus?

Pokud není váš problém uveden v seznamu výše, zkuste v nápovědě k produktu ESET Endpoint Antivirus 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.

- 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 Antivirus 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 ESET.

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 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. Více informací naleznete v ESET Databázi znalostí.

Jak produkty ESET zjistí, že je vyžadována jejich aktualizace? Z repozitáře? Odesílají se na servery nějaká data? 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/ESET Endpoint Antivirus uplatňováno nějaké omezení. Pokud ano, jak dlouho je 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. 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. Vzhledem k tomu, že funkce zajišťující automatickou aktualizaci je relativně nová, s největší pravděpodobností tento postup v budoucnosti rozvíjet za účelem zlepšení zkušenosti zákazníků.

Pokud spustím počítač v 8:45 a následně jej 17:00 vypnu, kdy dojde k automatické aktualizaci?

Při další úspěšné naplánované aktualizaci modulů, 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?

Aktuálně je možné automatickou aktualizaci vyvolat pouze kliknutím na tlačítko **Zkontrolovat aktualizace** v hlavním okně programu na záložce **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 Antivirus?

Aktualizaci ESET Endpoint Antivirus můžete provádět ručně nebo automaticky. Pro zahájení aktualizace klikněte na tlačítko **Zkontrolovat aktualizace** na záložce **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** (pro více informací přejděte do kapitoly Plánovač).

Jak aktivovat ESET Endpoint Antivirus?

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.).

Pro aktivaci ESET Endpoint Antivirus přejděte v hlavním okně programu na záložku **Nápověda a podpora** a klikněte na tlačítko **Aktivovat produkt**, případně na záložce **Stav ochrany** klikněte na odkaz **Aktivovat produkt**.

ESET Endpoint Antivirus 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 Business Account** – prostřednictvím účtu vytvořeného na portále ESET Business Account, do kterého se přihlásíte zadáním e-mailové adresy a hesla. K účtu se přihlásíte zadáním e-mailové adresy a hesla.
- **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. Pro více informací o generování offline licenčních souborů přejděte do online uživatelské příručky 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 a nevíte, jak ESET Endpoint Antivirus aktivovat, převeďte si je nejprve na licenční klíč.

Neúspěšná aktivace?

Kdykoli můžete licenci v produktu změnit. Pro přeaktivaci produktu jinou licencí přejděte v hlavním okně programu na záložku **Nápověda a podpora** a klikněte na tlačítko **Změnit licenci**. Na této obrazovce zároveň naleznete veřejné ID licence, které se používá pro identifikaci uživatele při komunikaci s technickou podporou společnosti ESET. Informaci o názvu počítače, tak jak jej vidí licenční portál, si zobrazíte kliknutím pravým tlačítkem myši na ikonu produktu v oznamovací oblasti a vybráním možnosti **O programu**.

Prostřednictvím ESET PROTECT 7.2 nebo ESET PROTECT 9 můžete aktivovat produkt vzdáleně a plně automaticky. Pro více informací přejděte do online nápovědy ESET PROTECT.

Zadání licenčního klíče během aktivace

Pro správný chod bezpečnostního produktu ESET Endpoint Antivirus 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.

Přihlášení k ESET Business Account

Účet Bezpečnostního administrátora je účet vytvořený na portále ESET Business Account, pomocí kterého můžete spravovat více licencí pohodlně z jednoho místa. Prostřednictvím účtu bezpečnostního administrátora můžete spravovat více licencí pohodlně z jednoho místa. Pokud ještě účet nemáte, po kliknutí na tlačítko **Vytvořit účet** budete přesměrováni na stránku, kde si nastavíte přihlašovací jméno a heslo k vašemu účtu na portále ESET Business Account.

Pokud jste zapomněli heslo ke svému účtu, klikněte na **Zapomněl jsem heslo** a budete přesměrování na portál ESET Business Account. Následně zadejte svoji e-mailovou adresu a potvrďte kliknutím na tlačítko **Odeslat**. Na e-mail následně obdržíte instrukce pro reset hesla.

Jak použít klasické licenční údaje pro aktivaci nové generace produktu ESET?

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.

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.

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 přejděte v hlavním okně programu na záložku **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 Antivirus k ESET PROTECT?

Pokud po instalaci ESET Endpoint Antivirus chcete počítač připojit k ESET PROTECT a spravovat jej vzdáleně, ujistěte se, že jste na stanici nainstalovali 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 Antivirus

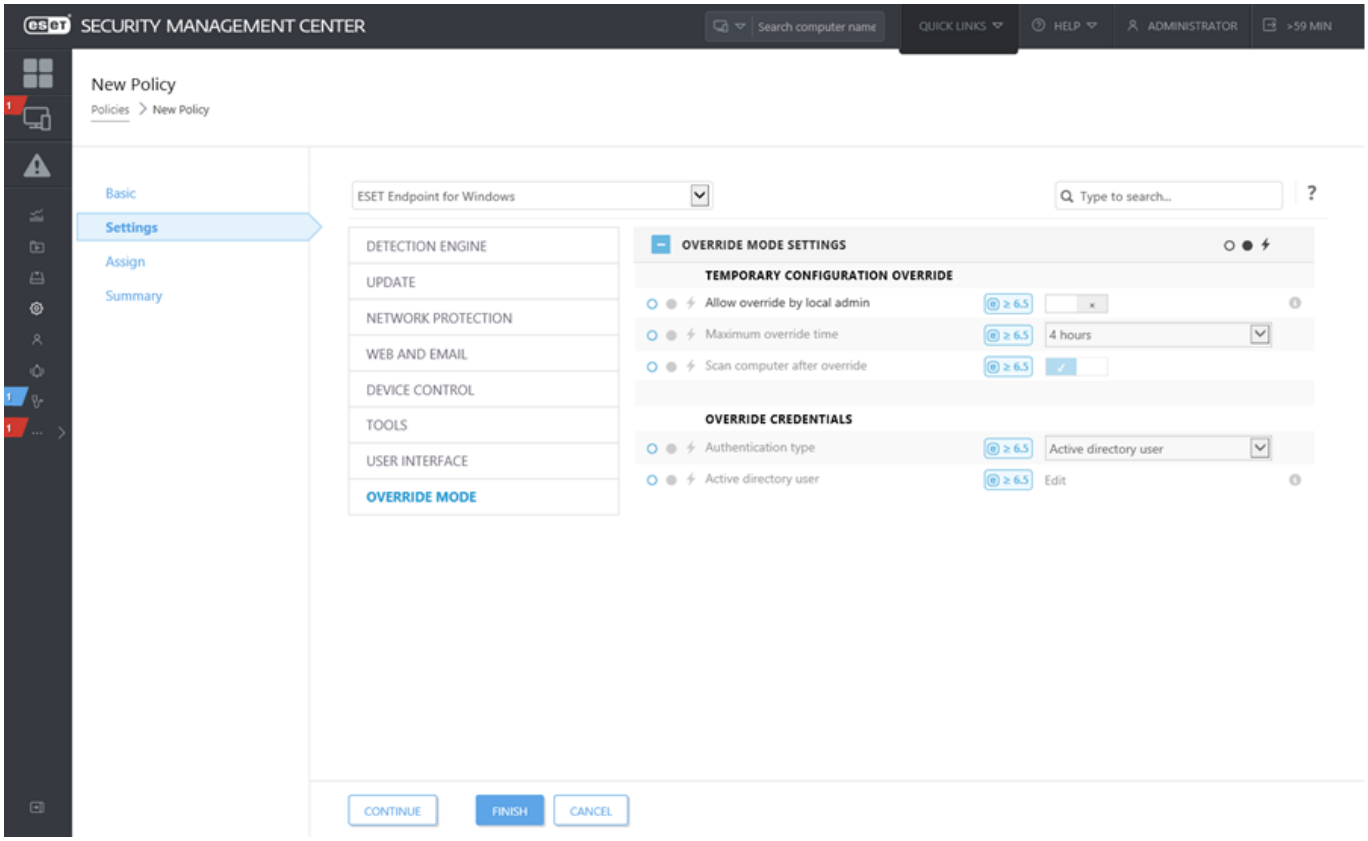
Jak dočasně změnit nastavení vynucené politikou?

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. 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 Antivirus.
• Od verze ESET Endpoint Antivirus 7.0.2100.4 můžete oprávnění definovat také na skupinu uživatelů z Active Directory.

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, kterou používá Filip, odebrat politiku, která mu umožnila dočasně měnit nastavení produktu.

Jak aplikovat doporučené politiky pro ESET Endpoint Antivirus

Po připojení ESET Endpoint Antivirus 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 Antivirus:

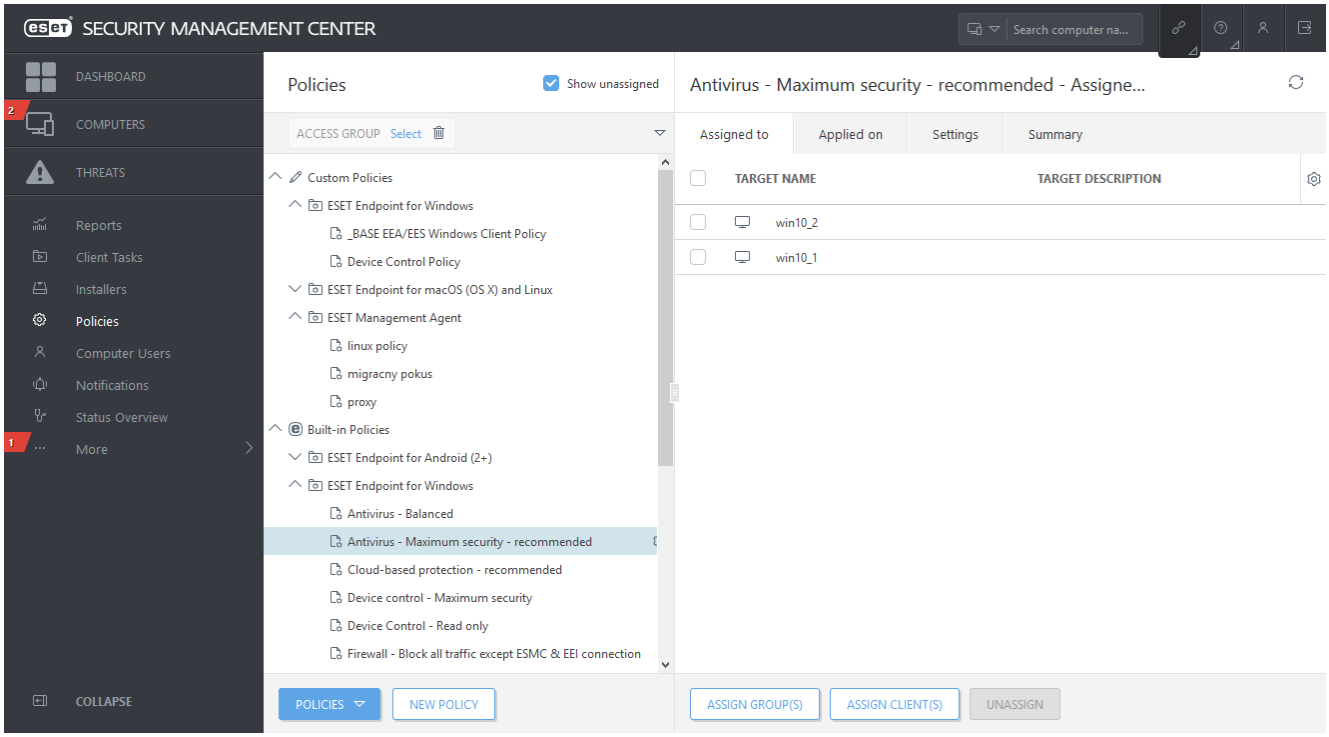
Politika	Popis
Antivirus – Vyvážené nastavení	Bezpečnostní konfigurace doporučená pro většinu situací.
Antivirus – Maximální zabezpečení	Aktivuje se strojové učení, rozšířená heuristika, hloubková analýza chování a filtrování protokolu SSL. Tyto funkce mají vliv na detekci potenciálně zneužitelných, 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 – Pouze 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. To vám usnadní řešení případných problémů. 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 Antivirus, 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 Antivirus prostřednictvím ESET PROTECT

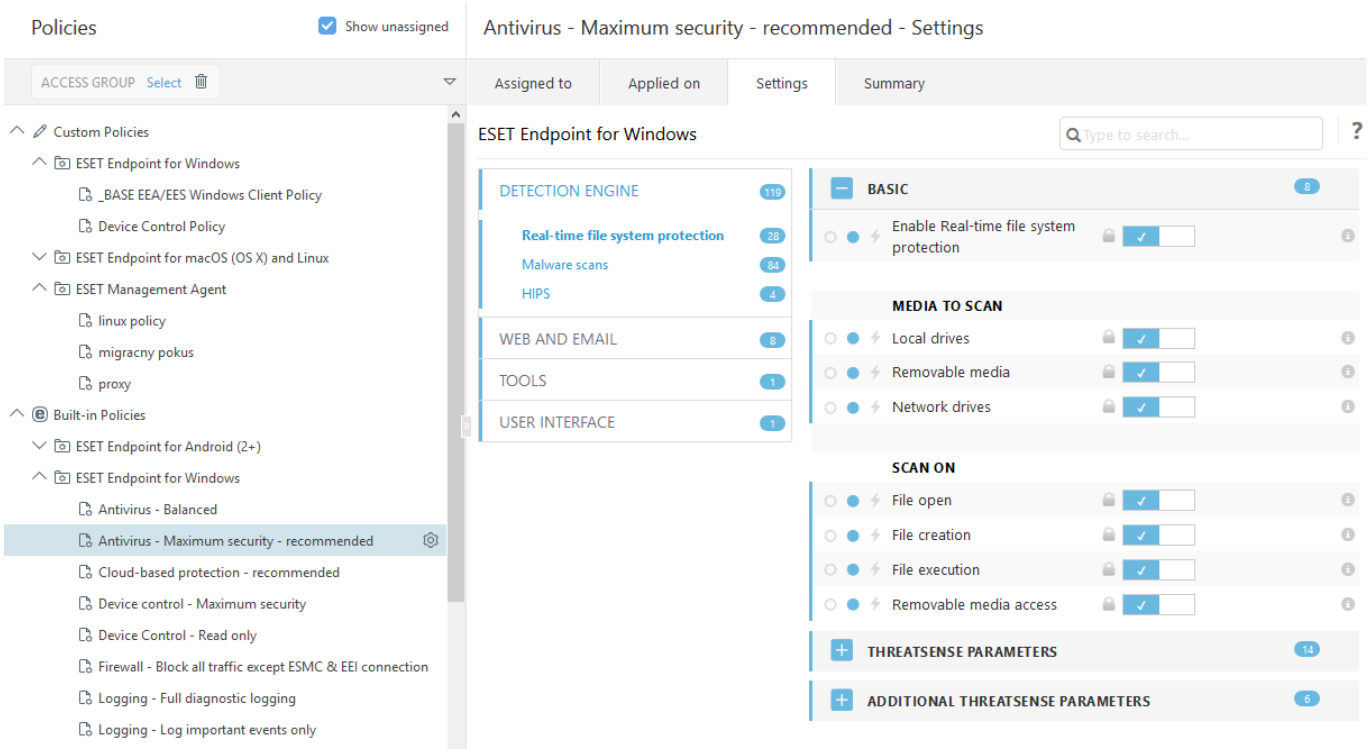
1. Otevřete si ESET PROTECT Web Console
2. V hlavním menu přejděte na záložku **Politiky** a rozbalte položku **Předdefinované politiky** > **ESET Endpoint for Windows**.
3. Klikněte na položku **Antivirus – Maximální zabezpečení – Doporučeno**.

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 Antivirus 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 Security nebo ESET Endpoint Antivirus.

Zpřístupnění aktualizačního mirroru prostřednictvím interního HTTP serveru poskytovaného produktem ESET Endpoint Antivirus

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 Antivirus?

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.

Verze 7.x:

Pro stažení nejnovější verze produktu ESET klikněte na jeden z níže uvedených odkazů v závislosti na používaném operačním systému a zakoupeném řešení ESET:

Stáhnout ESET Endpoint Security 7 32-bit Stáhnout ESET Endpoint Antivirus 7 32-bit

Stáhnout ESET Endpoint Security 7 64-bit Stáhnout ESET Endpoint Antivirus 7 64-bit

Verze 5.x:

Produkty z řady ESET Endpoint ve verzi 5.x jsou již na konce svého životního cyklu. To znamená, že již instalační balíčky nejsou veřejně dostupné ke stažení. Důrazně doporučujeme tyto produkty aktualizovat na nejnovější verzi.

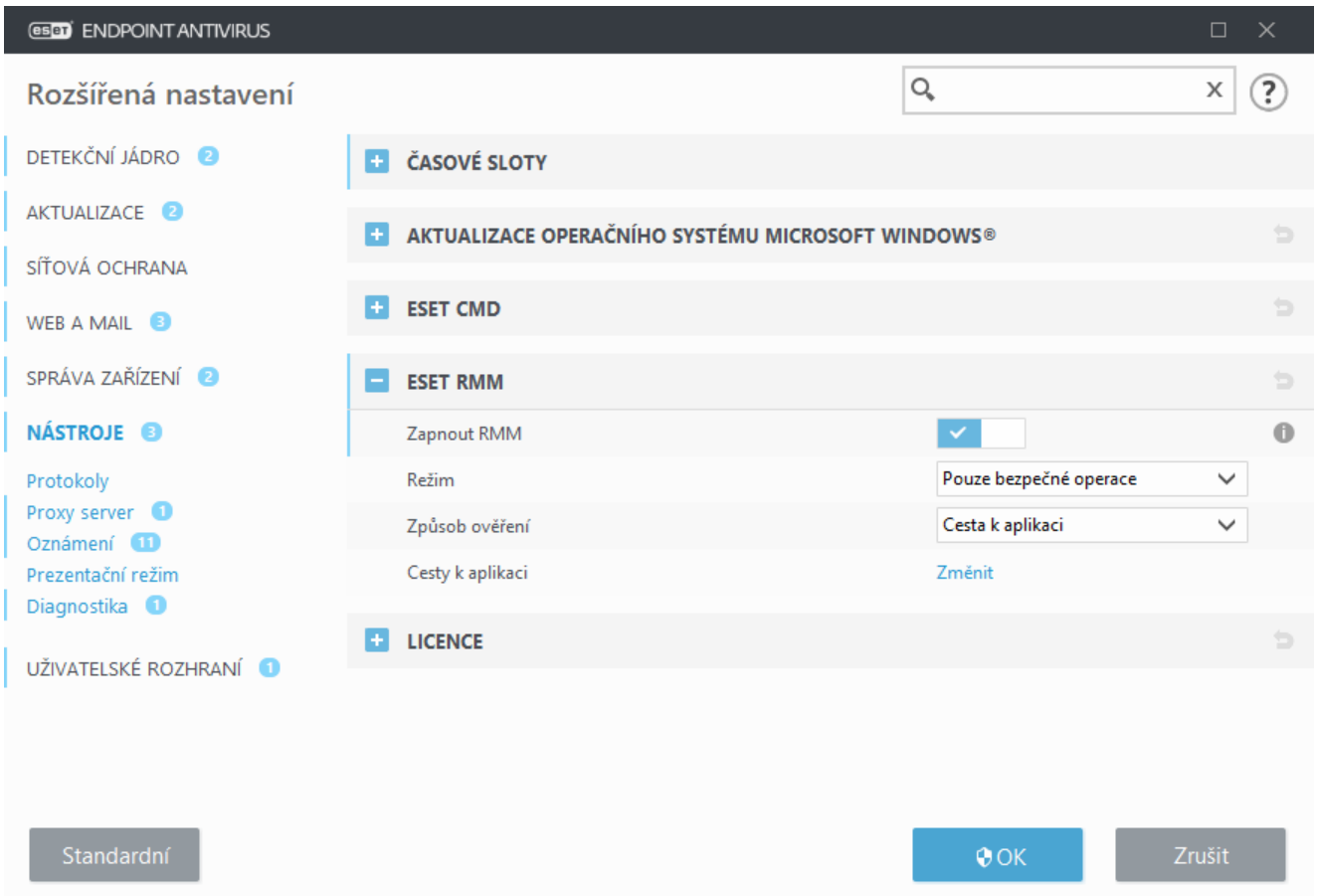
Další jazykové verze:

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 Antivirus podporuje správu prostřednictvím nástrojů třetích stran od verze 6.6.2028.0.



Standardně je ESET RMM vypnutý. Pro jeho aktivování přejděte v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu), přejděte do sekce **Nástroje** > **ESET RMM** a použijte přepínač **Zapnout RMM**.

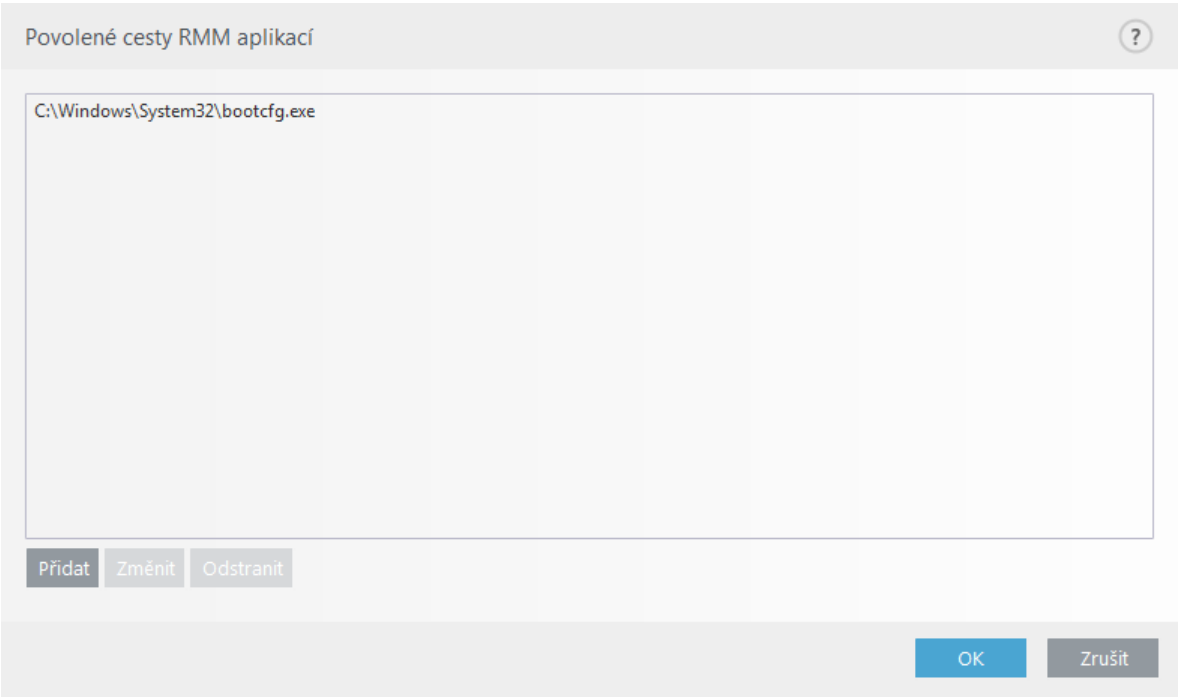
Režim – možnost **Pouze bezpečné operace** vyberte v případě, kdy RMM rozhraní chcete aktivovat pouze v režimu pro čtení a provádění bezpečných operací. Vybráním možnosti **Všechny operace** zajistíte provádění všech operací prostřednictvím RMM.

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.

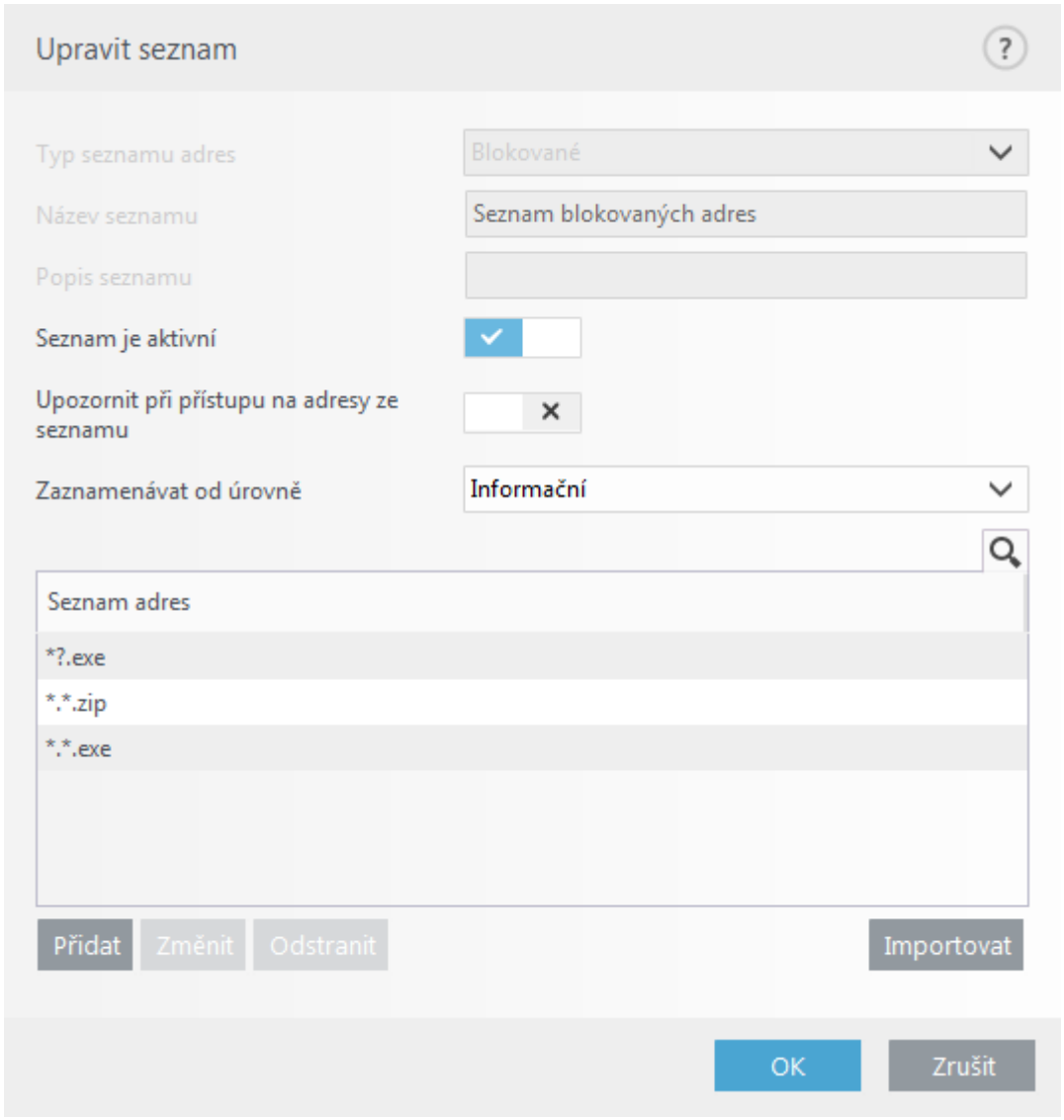
Soubor ermm.exe naleznete standardně ve složce s produktem ESET Endpoint Antivirus (například C*:\Program Files\ESET\ESET Security*. Binárka ermm.exe zajišťuje výměnu dat s RMM doplňkem, který komunikuje s RMM agentem, jenž je spojen s RMM serverem.

- 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?

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 zobrazeném dialogovém okně vyberte **seznam blokovaných adres** a klikněte na tlačítko **Změnit**, případně si kliknutím na tlačítko **Přidat** vytvořte seznam nový. Otevře se nové dialogové okno. Pokud si chcete vytvořit nový seznam, jako typ seznamu vyberte **Blokované**, a seznam pojmenujte. Dále si nastavte požadovanou hodnotu protokolování v rozbalovacím menu **Zaznamenávat od úrovně**. Dále z rozbalovacího menu vyberte úroveň, od které se budou **záznamy zapisovat do protokolu**. Do konzole pro vzdálenou správu se budou data přenášet v případě, kdy úroveň nastavíte na **Varování**.



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). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje jeden znak. Příklad: maska **/*.zip* zablokuje stahování všech .zip archivů, bez ohledu na zdroj.

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 Antivirus?

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.

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