

ESET Smart Security Premium

Uživatelská příručka

[Klikněte sem pro zobrazení online verze tohoto dokumentu](#)

Copyright ©2024 ESET, spol. s r.o.

ESET Smart Security Premium 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. 2024-04-12

1 ESET Smart Security Premium	1
1.1 Co je nového?	2
1.2 Jaký mám produkt?	2
1.3 Systémové požadavky	3
1.3 Zastaralá verze Microsoft Windows	4
1.4 Prevence	5
1.5 Návod programu	6
2 Instalace	7
2.1 Online instalační balíček	8
2.2 Offline instalace	9
2.2 Přejít na vyšší úroveň předplatného	11
2.2 Přejít na vyšší úroveň produktu	12
2.2 Přejít na nižší úroveň předplatného	12
2.2 Přejít na nižší úroveň produktu	13
2.3 Poradce při potížích s instalací	14
2.4 Prvotní kontrola počítače po dokončení instalace	14
2.5 Aktualizace na novou verzi	15
2.5 Automatická aktualizace starších produktů	16
2.5 Nainstaluje se ESET Smart Security Premium	16
2.5 Přejít na jinou produktovou řadu	16
2.5 Registrace	16
2.5 Průběh aktivace	17
2.5 Úspěšná aktivace	17
3 Jak začít	17
3.1 Ikona v oznamovací oblasti	17
3.2 Klávesové zkratky	18
3.3 Profily	18
3.4 Aktualizace	19
3.5 Nastavení ochrany sítě	21
3.6 Aktivace Anti-Theft	22
3.7 Rodičovská kontrola	23
4 Aktivace produktu	23
4.1 Zadání aktivačního klíče během aktivace	24
4.2 Použití účtu ESET HOME	24
4.3 Aktivovat zkušební verzi	25
4.4 Bezplatný aktivační klíč ESET	26
4.5 Neúspěšná aktivace - běžné scénáře	26
4.6 Stav předplatného	27
4.6 Neúspěšná aktivace z důvodu nadužívání předplatného	28
5 Práce s ESET Smart Security Premium	29
5.1 Přehled	30
5.2 Kontrola počítače	33
5.2 Spuštění volitelné kontroly	35
5.2 Průběh kontroly	37
5.2 Protokol kontroly počítače	39
5.3 Aktualizace	41
5.3 Dialogové okno - Vyžadován restart	43
5.3 Jak vytvořit aktualizací úlohu?	43
5.4 Nástroje	44
5.4 Protokoly	45

5.4 Filtrování protokolů	48
5.4 Spuštěné procesy	49
5.4 Bezpečnostní přehled	51
5.4 Síťová spojení	53
5.4 Síťová aktivita	54
5.4 ESET SysInspector	55
5.4 Plánovač	56
5.4 Možnosti naplánované kontroly	58
5.4 Informace o naplánované úloze	59
5.4 Detaily úlohy	59
5.4 Provedení úlohy	60
5.4 Provedení úlohy – Jednou	60
5.4 Provedení úlohy – Denně	60
5.4 Provedení úlohy – Týdně	60
5.4 Provedení úlohy – Při události	60
5.4 Neprovedení úlohy	61
5.4 Detaily úlohy – Aktualizace	61
5.4 Detaily úlohy – Spuštění aplikace	61
5.4 Kontrola systému	62
5.4 Strážce sítě	63
5.4 Síťové zařízení ve Strážci sítě	66
5.4 Oznámení Strážce sítě	67
5.4 Karanténa	67
5.4 Odeslání vzorku k analýze	70
5.4 Podezřelý soubor	71
5.4 Podezřelá stránka	71
5.4 Falešně detekovaný soubor	71
5.4 Falešně detekovaná stránka	72
5.4 Ostatní	72
5.5 Nastavení	72
5.5 Ochrana počítače	73
5.5 Nalezena infiltrace	75
5.5 Internetová ochrana	78
5.5 Anti-Phishingová ochrana	79
5.5 Rodičovská kontrola	80
5.5 Výjimky pro webové stránky	82
5.5 Kopírovat výjimky z účtu	84
5.5 Kopírovat kategorie z účtu	84
5.5 Síťová ochrana	84
5.5 Síťová spojení	86
5.5 Detaily síťového připojení	86
5.5 Řešení problémů s přístupem k síti	87
5.5 Seznam dočasně blokových IP adres	88
5.5 Protokoly síťové ochrany	89
5.5 Řešení problémů s Firewallem	89
5.5 Protokolování a vytváření pravidel nebo výjimek z protokolu	90
5.5 Vytvoření pravidla z protokolu	90
5.5 Vytváření výjimek z oznámení firewallu	90
5.5 Rozšířené protokolování síťové ochrany	91
5.5 Řešení problémů s Kontrolou síťové komunikace	91
5.5 Zablkovaná síťová hrozba	92

5.5 Zjištěno připojení do nové sítě	93
5.5 Navazování spojení – detekce	94
5.5 Změna aplikace	95
5.5 Příchozí důvěryhodná komunikace	95
5.5 Odchozí důvěryhodná komunikace	97
5.5 Příchozí komunikace	99
5.5 Odchozí komunikace	100
5.5 Možnosti zobrazení spojení	101
5.5 Bezpečnostní nástroje	102
5.5 Zabezpečené bankovníctví a prohlížení webu	102
5.5 Oznámení v prohlížeči	103
5.5 Ochrana soukromí a zabezpečení v prohlížeči	103
5.5 Anti-Theft	105
5.5 Přihlášení k účtu ESET HOME	107
5.5 Zadejte název zařízení	108
5.5 Anti-Theft je zapnutý/vypnutý	109
5.5 Přidání nového zařízení selhalo	109
5.5 Secure Data	109
5.5 Vytvořit šifrovaný virtuální disk	110
5.5 Zašifrovat soubory na výměnném médiu	111
5.5 Password Manager	111
5.5 Import a export nastavení	112
5.6 Nápověda a podpora	112
5.6 O programu ESET Smart Security Premium	113
5.6 ESET Novinky	114
5.6 Odeslat konfiguraci systému	115
5.6 Technická podpora	115
5.7 Účet ESET HOME	116
5.7 Připojení k ESET HOME	117
5.7 Přihlášení do ESET HOME	118
5.7 Neúspěšné přihlášení – běžné chyby	119
5.7 Přidání zařízení v ESET HOME	120
6 Rozšířená nastavení	120
6.1 Detekční jádro	121
6.1 Výjimky	122
6.1 Výkonnostní výjimky	122
6.1 Přidání a úprava výkonnostních výjimek	123
6.1 Formát výjimky podle cesty	125
6.1 Detekční výjimky	125
6.1 Přidání a úprava detekčních výjimek	127
6.1 Průvodce vytvořením detekční výjimky	128
6.1 Rozšířená nastavení detekčního jádra	129
6.1 Kontrola síťové komunikace	129
6.1 Cloudová ochrana	129
6.1 Filtr výjimek pro cloudovou ochranu	133
6.1 ESET LiveGuard	133
6.1 Detekce škodlivého kódu	135
6.1 Profily kontroly	135
6.1 Cíle kontroly	136
6.1 Kontrola při nečinnosti	136
6.1 Detekce stavu nečinnosti	137

6.1 Kontrola po startu	137
6.1 Automatická kontrola souborů spouštěných při startu počítače	137
6.1 Výměnná média	138
6.1 Ochrana dokumentů	139
6.1 HIPS – Host Intrusion Prevention System	140
6.1 HIPS výjimky	142
6.1 Rozšířená nastavení HIPS	142
6.1 Ovladače, jejichž načtení je vždy povoleno	143
6.1 Interaktivní režim HIPS	143
6.1 Učící režim skončil	144
6.1 Detekován potenciální ransomware	144
6.1 Správa HIPS pravidel	145
6.1 Úprava pravidla HIPS	146
6.1 Přidat cestu k aplikaci/registru pro HIPS	149
6.2 Aktualizace	149
6.2 Obnovení předchozí verze modulů	151
6.2 Interval pro obnovení předchozí verze modulů	153
6.2 Aktualizace produktu	153
6.2 Možnosti připojení	153
6.3 Ochrany	154
6.3 Rezidentní ochrana souborového systému	157
6.3 Vyloučené procesy	159
6.3 Přidání a úprava výjimek pro procesy	160
6.3 Kdy měnit nastavení rezidentní ochrany	160
6.3 Ověření funkčnosti rezidentní ochrany	160
6.3 Co dělat, když nefunguje rezidentní ochrana	161
6.3 Ochrana síťového připojení	161
6.3 Profily síťových připojení	162
6.3 Přidání nebo úprava profilů síťového připojení	163
6.3 Spouštěče	164
6.3 Sady IP adres	166
6.3 Úprava sad IP adres	166
6.3 Strážce sítě	167
6.3 Firewall	168
6.3 Nastavení učícího režimu	170
6.3 Pravidla firewallu	171
6.3 Přidání a úprava pravidel firewallu	172
6.3 Detekce změn aplikací	175
6.3 Seznam aplikací vyloučených z detekce	175
6.3 Ochrana proti síťovým útokům (IDS)	176
6.3 IDS pravidla	176
6.3 Ochrana proti útokům hrubou silou	179
6.3 Pravidla	180
6.3 Rozšířená nastavení	182
6.3 SSL/TLS	183
6.3 Pravidla pro kontrolu aplikací	185
6.3 Pravidla pro certifikáty	186
6.3 Šifrovaná síťová komunikace	187
6.3 Ochrana poštovních klientů	187
6.3 Ochrana transportu zpráv	188
6.3 Vyloučené aplikace	189

6.3 Vyloučené IP adresy	190
6.3 Ochrana poštovní schránky	191
6.3 Integrace	193
6.3 Panel nástrojů v MS Outlook	193
6.3 Potvrzovací dialog	194
6.3 Opakovaná kontrola zpráv	194
6.3 Reakce	194
6.3 Správa seznamů adres	195
6.3 Seznamy adres	196
6.3 Přidat/Upravit záznam	197
6.3 Výsledek zpracování adres	198
6.3 ThreatSense	198
6.3 Ochrana přístupu na web	201
6.3 Vyloučené aplikace	203
6.3 Vyloučené IP adresy	204
6.3 Správa seznamu URL adres	205
6.3 Seznam adres	206
6.3 Vytvoření nového seznamu URL adres	207
6.3 Jak přidat masku URL?	208
6.3 Kontrola HTTP(S) komunikace	209
6.3 ThreatSense	209
6.3 Rodičovská kontrola	212
6.3 Uživatelské účty	212
6.3 Nastavení uživatelského účtu	213
6.3 Kategorie	215
6.3 Ochrana prohlížeče	216
6.3 Zabezpečené bankovníctví a prohlížení webu	216
6.3 Správa zařízení	217
6.3 Editor pravidel ve správě zařízení	218
6.3 Detekovaná zařízení	219
6.3 Vytvoření nového pravidla	219
6.3 Skupiny zařízení	222
6.3 Ochrana webkamery	223
6.3 Editor pravidel ochrany webkamery	224
6.3 ThreatSense	224
6.3 Úrovně léčení	227
6.3 Přípony souborů vyloučených z kontroly	228
6.3 Doplnující parametry skenovacího jádra ThreatSense	228
6.4 Nástroje	229
6.4 Aktualizace operačního systému Windows	229
6.4 Dialogové okno – Aktualizace systému	230
6.4 Informace o aktualizacích	230
6.4 ESET CMD	230
6.4 Protokoly	232
6.4 Herní režim	233
6.4 Diagnostika	233
6.4 Technická podpora	235
6.5 Připojení	235
6.6 Uživatelské rozhraní	237
6.6 Prvky uživatelského rozhraní	237
6.6 Přístup k nastavení	238

6.6 Heslo pro přístup do Rozšířených nastavení	239
6.6 Podpora odečítačů obrazovky	239
6.7 Oznámení	240
6.7 Dialogová okna – Stavby aplikace	241
6.7 Oznámení na pracovní ploše	241
6.7 Seznam oznámení na pracovní ploše	242
6.7 Interaktivní upozornění	244
6.7 Potvrzovací zprávy	245
6.7 Přeposílání	246
6.8 Nastavení ochrany soukromí	249
6.8 Obnovit všechna nastavení na standardní	249
6.8 Obnovit všechna nastavení v této sekci na standardní	250
6.8 Chyba během ukládání nastavení	250
6.9 Skener příkazového řádku	250
7 FAQ	253
7.1 Jak aktualizovat ESET Smart Security Premium?	254
7.2 Jak odstranit vir z počítače?	254
7.3 Jak povolit komunikaci pro určitou aplikaci?	254
7.4 Jak zapnout rodičovskou kontrolu?	255
7.5 Jak vytvořit novou úlohu v Plánovači?	256
7.6 Jak naplánovat každý týden kontrolu počítače?	257
7.7 Jak obnovit přístup do rozšířených nastavení?	258
7.8 Jak deaktivovat produkt prostřednictvím portálu ESET HOME?	258
7.8 Produkt je deaktivovaný, zařízení je odpojené	259
7.8 Produkt není aktivován	259
8.1 Program zvyšování spokojenosti zákazníků	259
8.2 Licenční ujednání s koncovým uživatelem	260
8.3 Zásady ochrany osobních údajů	271

ESET Smart Security Premium

ESET Smart Security Premium představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ESET LiveGrid® v kombinaci s našimi vlastními moduly Firewall a Antispam rychle a přesně zajišťuje bezpečnost vašeho počítače. Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET Smart Security Premium 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 dopadu na výkon počítače nebo funkčnost operačního systému.

Funkce a přednosti

Přepřacované uživatelské rozhraní	Uživatelské rozhraní produktu bylo kompletně přepřacováno. Nyní je čistější, přehlednější a intuitivnější. Upravili jsme textaci oznámení zobrazených uživateli a přidali také podporu pro jazyky se zápisem zprava doleva, jako je hebrejščina a arabština. Prostřednictvím online nápovědy, integrované do produktu, získáte vždy nejaktuálnější informace ke konkrétním zobrazeným oknům v programu ESET Smart Security Premium.
Tmavý režim	Rozšíření pro zapnutí tmavého zobrazení uživatelského rozhraní. Preferované barevné schéma si můžete zvolit v prvcích uživatelského rozhraní .
Antivirus a antispyware	Proaktivně detekuje a léčí známé i neznámé viry, červy, trojské koně a rootkity. Pokročilá heuristika označí každý dosud neznámý škodlivý kód, chrání vás před neznámými hrozbami a eliminuje je dříve, než mohou způsobit škodu. Ochrana přístupu na web a anti-phishingová ochrana monitorují komunikaci mezi webovými prohlížeči 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 Smart Security Premium vůči cloudové databázi.
Správa zařízení	Produkt automaticky kontroluje všechny USB disky, paměťové karty a CD/DVD. Dále dokáže blokovat výměnná média podle typu, výrobce, velikosti a dalších atributů.
HIPS	Pomocí tohoto modulu si můžete přizpůsobit detailní chování systému a jeho bezpečnost pomocí pravidel pro systémový registr, aktivní procesy a programy.
Herní režim	Odloží všechna vyskakovací okna, aktualizace nebo jiné činnosti náročné na systém, aby šetřil systémové prostředky pro hraní her a jiné činnosti na celé obrazovce.

Funkce ESET Smart Security Premium

Zabezpečené bankovníctví a prohlížení webu	Zabezpečené bankovníctví a prohlížení webu nabízí zabezpečení prohlížeče pro přístup k online bankovníctví nebo online platebním branám, aby všechny online transakce probíhaly v důvěryhodném a bezpečném prostředí.
Podpora síťových vzorků	Síťové podpisy umožňují rychlou identifikaci a blokování škodlivé komunikace přicházející z uživatelských zařízení nebo na ně směřující, například botů a balíčků exploitů. Jedná se o funkci ochrany proti zapojení do botnetu.

Inteligentní firewall	Modul firewall kontroluje síťovou komunikaci a chrání počítač před neautorizovaným přístupem.
Antispamová ochrana poštovních klientů	Spam představuje více než 50 % veškeré e-mailové komunikace. Antispamová ochrana poštovních klientů chrání před tímto problémem.
Anti-Theft	Anti-Theft výrazně rozšiřuje možnosti zabezpečení zařízení v případě ztráty nebo odcizení. Pokud si na zařízení nainstalujete ESET Smart Security Premium a zapnete funkci Anti-Theft, zařízení se ve stejnojmenné části ESET HOME zobrazí. Pomocí webového rozhraní můžete na zařízení konfigurovat a spravovat funkce Anti-Theft, např. označit zařízení za ztracené nebo jej vzdáleně ovládat.
Rodičovská kontrola	Zabrání vašim potomkům v přístupu na stránky s nevhodným obsahem.
Password Manager	Správce hesel chrání vaše osobní údaje a pamatuje si za vás hesla.
Šifrování dat	Prostřednictvím funkce Secure Data můžete šifrovat data ve svém počítači a na výměnných médiích, čímž zabráníte zneužití osobních a citlivých údajů.
ESET LiveGuard	Bezpečnostní vrstva, která odhaluje a blokuje dosud neznámé hrozby a zpracovává informace pro jejich budoucí detekci.

Aby ESET Smart Security Premium fungoval správně, musí být předplatné aktivní. Doporučujeme obnovit předplatné několik týdnů před jeho vypršením pro ESET Smart Security Premium.

Co je nového?

Co je nového v ESET Smart Security Premium verze 17.1

- Drobná vylepšení Strážce sítě
- Drobná vylepšení Zabezpečeného bankovníctví a prohlížení webu
- ESET LiveGuard – odesílání dokumentů je nyní ve výchozím nastavení zapnuto
- Další drobné opravy a vylepšení

Jak vypnout **oznámení Co je nového**:

1. Otevřete [Rozšířená nastavení](#) > **Oznámení** > **Oznámení na pracovní ploše**.
2. Klikněte na **Změnit** vedle položky **Oznámení na pracovní ploše**.
3. Zrušte zaškrtnutí políčka **Zobrazovat oznámení Co je nového** a klikněte na tlačítko **OK**. Více informací naleznete v [samostatné kapitole](#).

i Podrobný seznam změn v ESET Smart Security Premium naleznete v [seznamu změn ESET Smart Security Premium](#).

Jaký mám produkt?

ESET nabízí více vrstev zabezpečení s novými produkty od výkonného a rychlého antivirového řešení až po komplexní bezpečnostní řešení s minimálním dopadem na výkon systému:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**

- ESET Smart Security Premium

- ESET Security Ultimate

Pro zjištění, jaký produkt máte nainstalován, si otevřete [hlavní okno programu](#) a podívejte se do levého horního rohu (viz článek v [Databázi znalostí](#)).

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekční jádro	✓	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓	✓
Exploit Blocker	✓	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓	✓
Antispam		✓	✓	✓
Firewall		✓	✓	✓
Strážce sítě		✓	✓	✓
Ochrana webkamery		✓	✓	✓
Ochrana proti síťovým útokům		✓	✓	✓
Ochrana proti zapojení do botnetu		✓	✓	✓
Zabezpečené bankovníctví a prohlížení webu		✓	✓	✓
Ochrana soukromí a zabezpečení v prohlížeči		✓	✓	✓
Rodičovská kontrola		✓	✓	✓
Anti-Theft		✓	✓	✓
Password Manager			✓	✓
ESET Secure Data			✓	✓
ESET LiveGuard			✓	✓
VPN				✓
Identity Protection				✓

i Některé výše uvedené produkty nemusí být k dispozici pro váš jazyk / region.

Systémové požadavky

Pro plynulý běh ESET Smart Security Premium by váš systém měl splňovat následující 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

Podporované operační systémy

Microsoft® Windows® 11

Microsoft® Windows® 10



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



Vždy se snažte udržovat svůj operační systém aktualizovaný.

Požadavky funkcí produktu ESET Smart Security Premium

V tabulce níže naleznete systémové požadavky pro konkrétní funkce ESET Smart Security Premium:

Funkce	Požadavky
Intel® Threat Detection Technology	Viz podporované procesory .
Zabezpečené bankovníctví a prohlížení webu	Viz podporované prohlížeče .
Průhledné pozadí	Verze systému Windows 10 RS4 a novější.
ESET Specialized Cleaner	Procesor nezaložený na architektuře ARM64.
Kontrola systému	Procesor nezaložený na architektuře ARM64.
Exploit Blocker	Procesor nezaložený na architektuře ARM64.
Hlubková analýza chování	Procesor nezaložený na architektuře ARM64.

Ostatní

Pro aktivaci ESET Smart Security Premium a získání aktualizací pro jeho správnou funkci je vyžadováno internetové připojení.

Souběžné používání dvou antivirových programů na jednom zařízení povede nevyhnutelně ke konfliktu v přístupu k systémovým prostředkům, což se projeví zpomalením zařízení a může vést i k jeho nefunkčnosti.

Zastaralá verze Microsoft Windows

Problém

- Pokoušíte se nainstalovat nejnovější verzi ESET Smart Security Premium na zařízeních s Windows 7, Windows 8 (8.1) nebo Windows Home Server 2011
- ESET Smart Security Premium při instalaci zobrazí chybu **Zastaralý operační systém**

Detaily

Nejnovější verze ESET Smart Security Premium vyžaduje operační systém Windows 10 nebo Windows 11.

Řešení

K dispozici jsou následující možnosti:

Přejít na Windows 10 nebo Windows 11

Proces aktualizace je poměrně jednoduchý. Pouze zřídka dochází ke ztrátě dat. Před aktualizací na Windows 10:

1. Proveďte zálohu svých dat.
2. Pročtěte si na stránkách společnosti Microsoft [často kladené otázky k aktualizaci na Windows 10](#) nebo [často kladené otázky k aktualizaci na Windows 11](#) a následně proveďte aktualizaci operačního systému Windows.

Instalace ESET Smart Security Premium verze 16.0

Pokud nemůžete aktualizovat systém Windows, [nainstalujte si ESET Smart Security Premium ve verzi 16.0](#). Další informace naleznete v [online příručce k ESET Smart Security Premium ve verzi 16.0](#).

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. Analytici z ESET Research Lab analyzují tyto hrozby a vydávají aktualizace denně, 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 potenciálních nákaz. Je důležité stáhnout aktualizace zabezpečení co nejdříve po jejich vydání. Microsoft Windows a webové prohlížeče, jako např. Internet Explorer, jsou dva příklady programů, pro které jsou vydány aktualizace zabezpečení v pravidelném rozvrhu.

Zálohování důležitých dat

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

nutné. Výrazně tím usnadníte a urychlíte případnou obnovu dat po pádu systému.

Pravidelná kontrola počítače

Detekci známých i neznámých virů, červů, trojských koní a rootkitů zajišťuje rezidentní ochrana souborového systému. 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 uživatelském manuálu ESET Smart Security Premium. Věříme, že informace obsažené v této nápovědě vás seznámí s produktem a pomohou vám zabezpečit počítač.

Jak začít

Před použitím ESET Smart Security Premium vám doporučujeme seznámit se s různými [typy infiltrací](#) a [útoků na dálku](#), se kterými se můžete setkat. O nových funkcích v ESET Smart Security Premium si můžete přečíst v [samostatné kapitole](#).


Začněte kapitolou [Instalace ESET Smart Security Premium](#). Pokud již máte ESET Smart Security Premium nainstalovaný, přečtěte si kapitolu [Práce s ESET Smart Security Premium](#).


Jak používat nápovědu programu ESET Smart Security Premium


Témata Online nápovědy jsou rozdělena do několika kapitol a podkapitol. Pokud si s konkrétní částí produktu ESET Smart Security Premium nevíte rady, stiskněte funkční klávesu **F1** a zobrazí se vám nápověda.


Online nápověda umožňuje vyhledávání prostřednictvím klíčových slov nebo pomocí slovních spojení. 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.

Připravili jsme také průvodce, který vám pomůže se základním nastavením ESET Smart Security Premium. 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 ukázkou pro pochopení fungování nebo používání dané funkce.


Konvence	Význam
Tučné písmo	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.
<i>Kurzíva</i>	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 nápovědy.

Instalace

Instalaci ESET Smart Security Premium můžete na svém počítači provést dvěma způsoby. Způsoby instalace se mohou lišit v závislosti na zemi a způsobu vydání:

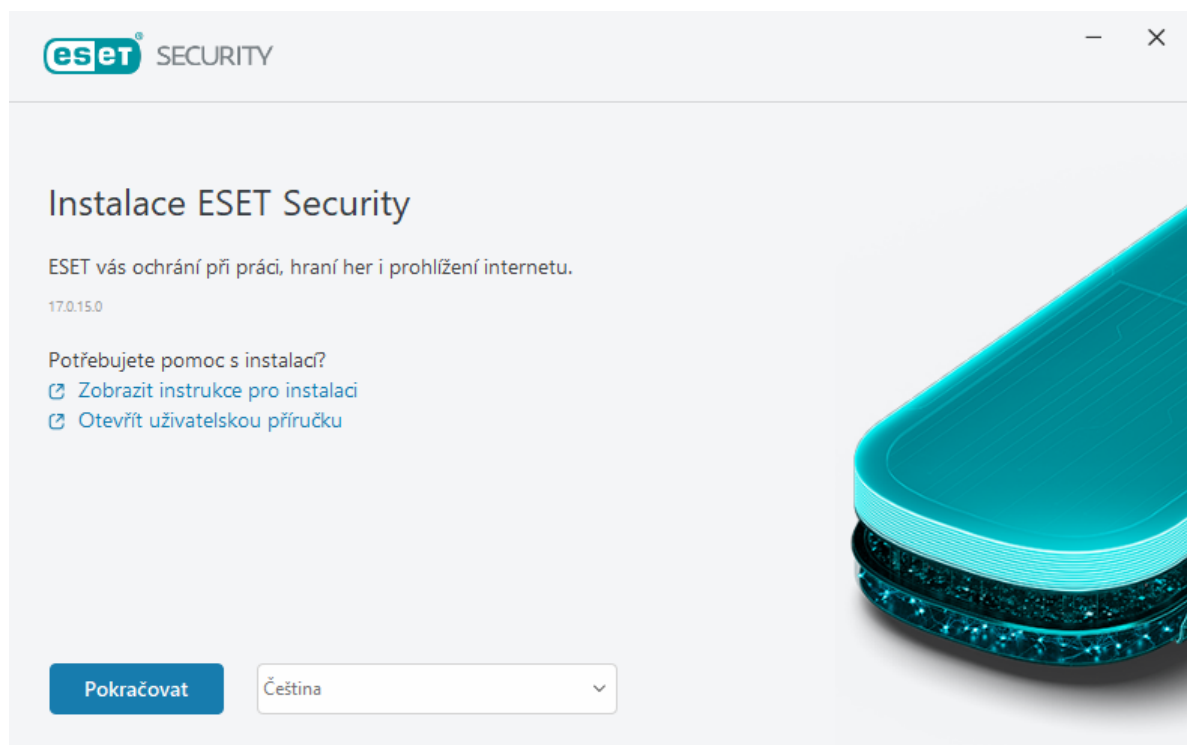
- [Live installer](#) si můžete stáhnout z internetových stránek společnosti ESET, případně jej naleznete na zakoupeném CD/DVD. Instalační balíček je univerzální pro všechny jazykové varianty (při instalaci vyberete jazykovou verzi). Jedná se o malý soubor. Další potřebné soubory pro instalaci ESET Smart Security Premium se stáhnou automaticky z internetu.
- [Offline instalační balíček](#) – jedná se o .exe soubor, který obsahuje všechny soubory potřebné pro instalaci. Proto je větší než Live installer a nevyžaduje připojení k internetu.

 Před spuštěním instalace ESET Smart Security Premium se ujistěte, že na počítači není nainstalován žádný jiný 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 [ESET Databázi znalostí](#) naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů (dostupný v angličtině a několika dalších jazycích).

Online instalační balíček

Po stažení [Online instalačního balíčku](#) dvakrát klikněte na instalační soubor a postupujte podle pokynů v Průvodci instalací.

! Tento způsob instalace vyžaduje připojení k internetu.



1. Z rozbalovacího menu vyberte požadovanou jazykovou verzi a klikněte na tlačítko **Pokračovat**.

i Pokud již máte v počítači nainstalovanou starší verzi programu, ve které je nastavení chráněno heslem, je třeba heslo zadat. O heslu chráněného přístupu do nastavení si přečtěte v kapitole [Přístup k nastavení](#).

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

- [Systém zpětné vazby ESET LiveGrid®](#)
- [Potenciálně nechtěné aplikace](#)
- [Program zvyšování spokojenosti zákazníků](#)

i Kliknutím na tlačítko **Pokračovat** nebo **Povolit vše a pokračovat** souhlasíte se zněním Licenčního ujednání s koncovým uživatelem a berete na vědomí Zásady ochrany osobních údajů.

3. Pokud chcete produkt aktivovat, spravovat a sledovat jeho bezpečnostní stav prostřednictvím portálu ESET HOME, [připojte zařízení ke svému účtu ESET HOME](#). Chcete-li pokračovat bez připojení, klikněte na **Přeskočit přihlášení**. Zařízení můžete [připojit k účtu ESET HOME](#) kdykoli později.

4. Pokud budete pokračovat bez připojení k účtu ESET HOME, zvolte si [možnost aktivace](#). Pokud již máte v

počítači nainstalovanou starší verzi programu, **aktivační klíč** se převezme automaticky.

5. Na základě vašeho předplatného průvodce instalací zjistí, který ESET produkt má nainstalovat. Vždy se předvybere produkt, který obsahuje nejvíce bezpečnostních funkcí. Pokud si přejete [nainstalovat jiný bezpečnostní produkt ESET](#), klikněte na možnost **Změnit produkt**. Kliknutím na tlačítko **Pokračovat** spustíte instalaci. Může to chvíli trvat.

i Pokud by se v počítači nacházely v minulosti neodinstalované části produktů ESET (soubory nebo složky), budete vyzváni k jejich odstranění. Pro pokračování klikněte na tlačítko **Instalovat**.

6. Kliknutím na tlačítko **Dokončit** ukončíte Průvodce instalací.

! [Poradce při potížích s instalací](#).

i Po dokončení instalace a aktivování produktu se zahájí stahování aktualizací modulů. V tuto chvíli se teprve začnou inicializovat moduly ochrany a některé funkce nemusí být do dokončení aktualizace dostupné.

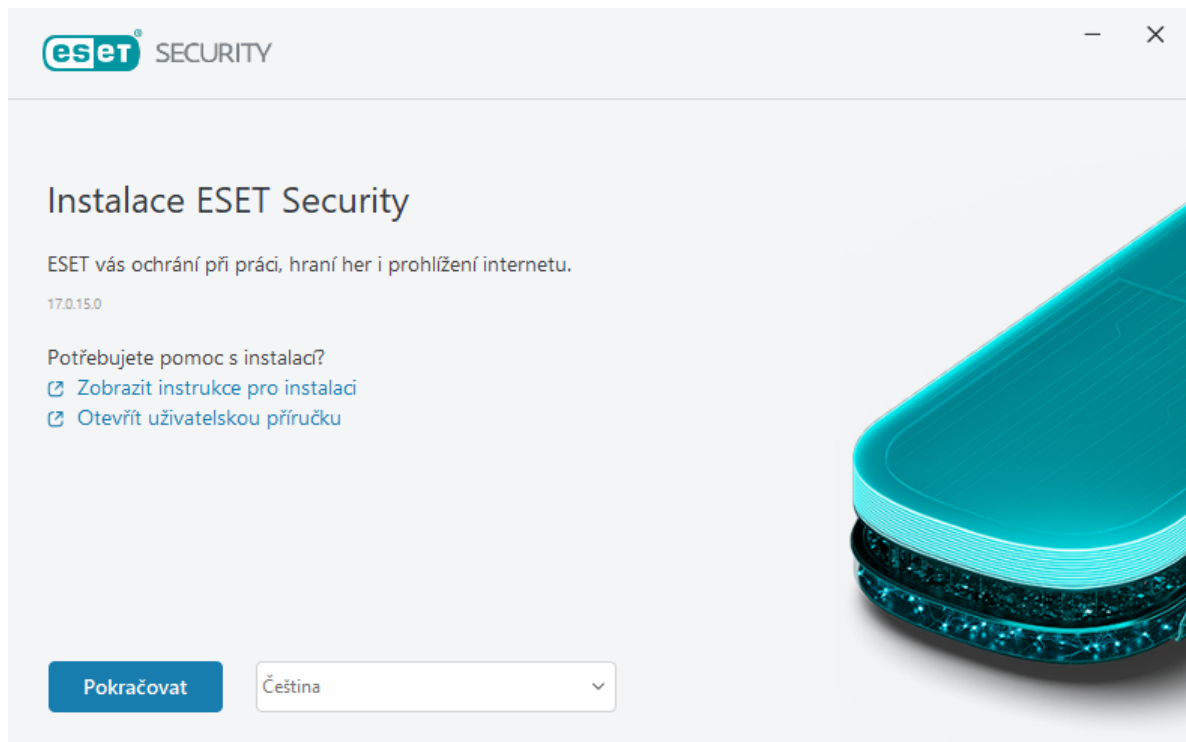
Offline instalace

Pomocí níže uvedeného odkazu si stáhněte offline instalační balíček (.exe) a nainstalujte produkt ESET určený pro domácí uživatele na platformě Windows. [Vyberte si, kterou verzi produktu ESET pro domácnosti chcete stáhnout](#) (32bitovou, 64bitovou nebo ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Stáhnout 64-bitový balíček	Stáhnout 64-bitový balíček	Stáhnout 64-bitový balíček	Stáhnout 64bitový balíček
Stáhnout 32-bitový balíček	Stáhnout 32-bitový balíček	Stáhnout 32-bitový balíček	Stáhnout 32bitový balíček
Stáhnout ARM balíček	Stáhnout ARM balíček	Stáhnout ARM balíček	Stáhnout ARM balíček

! Pokud máte dostupné připojení k internetu, doporučujeme pro instalaci bezpečnostního produktu ESET využít [online instalační balíček](#).

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



1. Z rozbalovacího menu vyberte požadovanou jazykovou verzi a klikněte na tlačítko **Pokračovat**.

i Pokud již máte v počítači nainstalovanou starší verzi programu, ve které je nastavení chráněno heslem, je třeba heslo zadat. O heslu chránícího přístup do nastavení si přečtete v kapitole [Přístup k nastavení](#).

2. Vyberte, zda chcete využívat následující funkce, přečtete si [Licenční ujednání s koncovým uživatelem](#) a [Zásady ochrany osobních údajů](#). Klikněte na tlačítko **Pokračovat**, případně klikněte na **Povolit vše a pokračovat**, čímž zapnete funkce:

- [Systém zpětné vazby ESET LiveGrid®](#)
- [Potenciálně nechtěné aplikace](#)
- [Program zvyšování spokojenosti zákazníků](#)

i Kliknutím na tlačítko **Pokračovat** nebo **Povolit vše a pokračovat** souhlasíte se zněním Licenčního ujednání s koncovým uživatelem a berete na vědomí Zásady ochrany osobních údajů.

3. Dále klikněte na **Přeskočit přihlášení**. Pokud jste však připojeni k internetu, můžete zařízení rovnou [připojit ke svému ESET HOME účtu](#).

4. Dále klikněte na **Přeskočit aktivaci**. Aby byl produkt ESET Smart Security Premium funkční, je nutné jej po dokončení instalace aktivovat. Pro jeho [aktivaci](#) je vyžadováno připojení k internetu.

5. V dalším kroku se zobrazí informace, který bezpečnostní produkt ESET se nainstalujete (dle staženého offline instalačního balíčku). Kliknutím na tlačítko **Pokračovat** spustíte instalaci. Může to chvíli trvat.

i Pokud by se v počítači nacházely v minulosti neodinstalované části produktů ESET (soubory nebo složky), budete vyzváni k jejich odstranění. Pro pokračování klikněte na tlačítko **Instalovat**.

6. Kliknutím na tlačítko **Dokončit** ukončíte Průvodce instalací.

Přechod na vyšší úroveň předplatného

Toto oznamovací okno se zobrazí v případě, že došlo ke změně předplatného použitého pro aktivaci produktu ESET. Nové předplatné vám umožní aktivovat produkt s více bezpečnostními funkcemi. Pokud neprovedete žádnou akci, ESET Smart Security Premium zobrazí se okno **Změna na produkt s vyšším množstvím bezpečnostních funkcí**.

Ano (doporučeno) – automaticky nainstaluje produkt s větším množstvím bezpečnostních funkcí.

Ne, děkuji – nebudou provedeny žádné změny a oznámení trvale zmizí.

Pro pozdější změnu produktu si prostudujte článek [Jak změnit domácí produkt bez odinstalace původního](#)? Více informací o předplatném ESET naleznete v sekci [Často kladené dotazy k předplatnému](#).

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekční jádro	✓	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓	✓
Exploit Blocker	✓	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓	✓
Antispam		✓	✓	✓
Firewall		✓	✓	✓
Strážce sítě		✓	✓	✓
Ochrana webkamery		✓	✓	✓
Ochrana proti síťovým útokům		✓	✓	✓
Ochrana proti zapojení do botnetu		✓	✓	✓
Zabezpečené bankovníctví a prohlížení webu		✓	✓	✓
Ochrana soukromí a zabezpečení v prohlížeči		✓	✓	✓
Rodičovská kontrola		✓	✓	✓
Anti-Theft		✓	✓	✓
Password Manager			✓	✓
ESET Secure Data			✓	✓
ESET LiveGuard			✓	✓
VPN				✓
Identity Protection				✓

Povýšení produktu

Stáhli jste si výchozí instalační balíček a rozhodli jste se změnit produkt, který se má aktivovat nebo chcete změnit nainstalovaný produkt na produkt s větším množstvím bezpečnostních funkcí.

[Jak změnit produkt v průběhu instalace?](#)

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekční jádro	✓	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓	✓
Exploit Blocker	✓	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓	✓
Antispam		✓	✓	✓
Firewall		✓	✓	✓
Strážce sítě		✓	✓	✓
Ochrana webkamery		✓	✓	✓
Ochrana proti síťovým útokům		✓	✓	✓
Ochrana proti zapojení do botnetu		✓	✓	✓
Zabezpečené bankovníctví a prohlížení webu		✓	✓	✓
Ochrana soukromí a zabezpečení v prohlížeči		✓	✓	✓
Rodičovská kontrola		✓	✓	✓
Anti-Theft		✓	✓	✓
Password Manager			✓	✓
ESET Secure Data			✓	✓
ESET LiveGuard			✓	✓
VPN				✓
Identity Protection				✓

Přechod na nižší úroveň předplatného

Toto dialogové okno se zobrazí v případě, že došlo ke změně předplatného použitého pro aktivaci produktu ESET. Nové předplatné můžete používat pouze s jiným produktem ESET s menším počtem bezpečnostních funkcí. Aby nedošlo ke ztrátě ochrany, byl produkt automaticky změněn.

Více informací o předplatném ESET naleznete v sekci [Často kladené dotazy k předplatnému](#).

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekční jádro	✓	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓	✓
Exploit Blocker	✓	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓	✓
Antispam		✓	✓	✓
Firewall		✓	✓	✓
Strážce sítě		✓	✓	✓
Ochrana webkamery		✓	✓	✓
Ochrana proti síťovým útokům		✓	✓	✓
Ochrana proti zapojení do botnetu		✓	✓	✓
Zabezpečené bankovníctví a prohlížení webu		✓	✓	✓
Ochrana soukromí a zabezpečení v prohlížeči		✓	✓	✓
Rodičovská kontrola		✓	✓	✓
Anti-Theft		✓	✓	✓
Password Manager			✓	✓
ESET Secure Data			✓	✓
ESET LiveGuard			✓	✓
VPN				✓
Identity Protection				✓

Ponížení produktu

Produkt, který jste právě nainstalovali, má více bezpečnostních funkcí než ten, který se chystáte aktivovat. Password Manager a funkce Šifrování dat nejsou součástí tohoto produktu. Nebudete tedy moci vytvářet šifrované soubory.

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekční jádro	✓	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓	✓
Exploit Blocker	✓	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
HIPS (včetně ochrany proti ransomware)	✓	✓	✓	✓
Antispam		✓	✓	✓
Firewall		✓	✓	✓
Strážce sítě		✓	✓	✓
Ochrana webkamery		✓	✓	✓
Ochrana proti síťovým útokům		✓	✓	✓
Ochrana proti zapojení do botnetu		✓	✓	✓
Zabezpečené bankovníctví a prohlížení webu		✓	✓	✓
Ochrana soukromí a zabezpečení v prohlížeči		✓	✓	✓
Rodičovská kontrola		✓	✓	✓
Anti-Theft		✓	✓	✓
Password Manager			✓	✓
ESET Secure Data			✓	✓
ESET LiveGuard			✓	✓
VPN				✓
Identity Protection				✓

Poradce při potížích s instalací

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

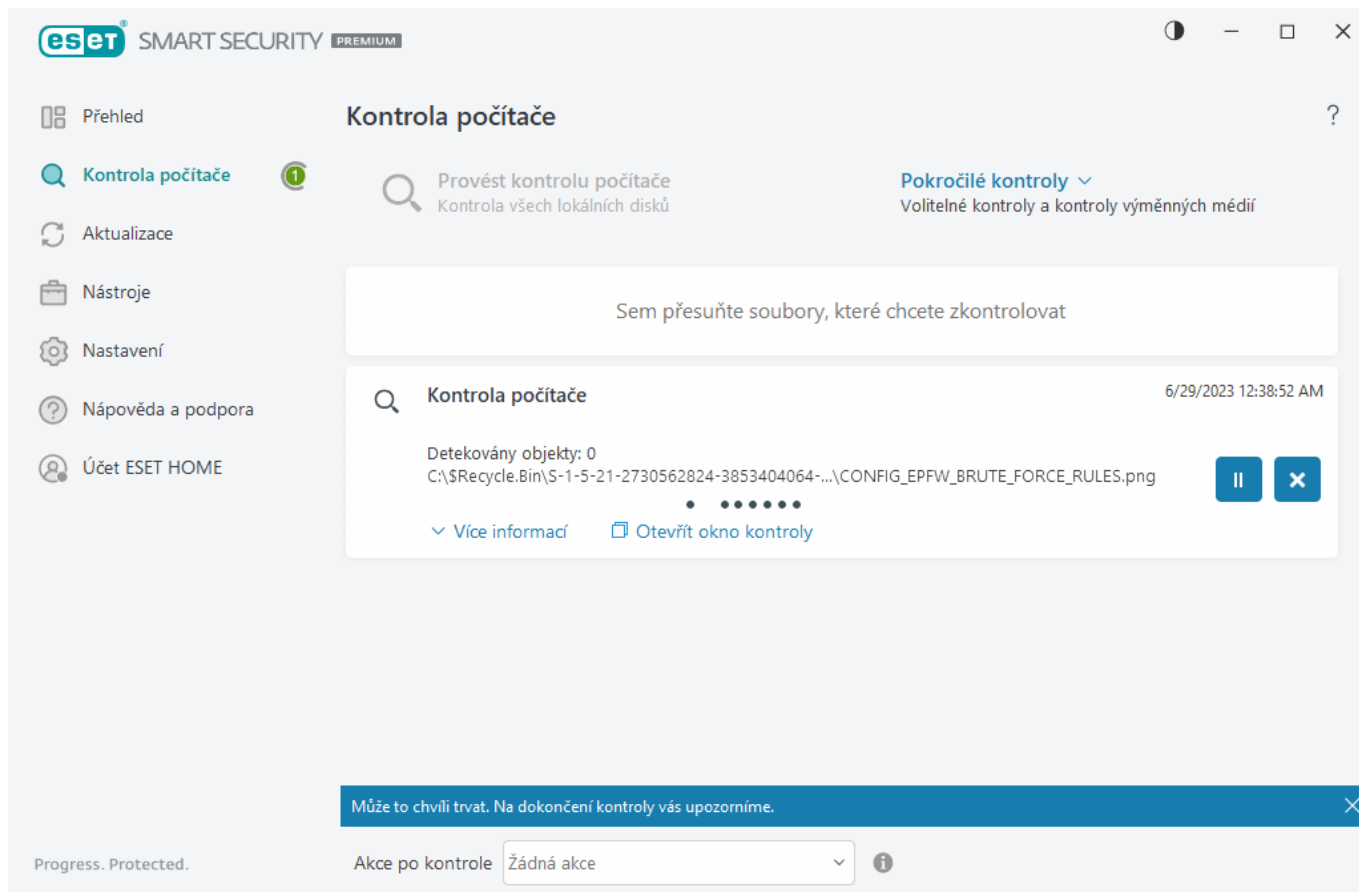
Pro spuštění klikněte na **Spustit Poradce při potížích**. Po dokončení postupujte podle doporučeného řešení.

Pokud problém přetrvává, podívejte se na seznam [Známých chyb při instalaci a jejich řešení](#).

Prvotní kontrola počítače po dokončení instalace

Po nainstalování ESET Smart Security Premium a aktualizování detekčních modulů se spustí automatická kontrola počítače zajišťující ochranu před škodlivým kódem.

Kontrolu počítače můžete spustit také kdykoli ručně kliknutím v [hlavním okně programu](#) na záložku **Kontrola počítače** > **Provést kontrolu počítače**. Více informací naleznete v kapitole [Kontrola počítače](#).



Aktualizace na novou verzi

Nové verze ESET Smart Security Premium 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 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 jste povolili **Aktualizace programových funkcí** v [Rozšířených nastaveních](#) > **Aktualizace** > **Profily** > **Aktualizace**.

2. Ručně – v [hlavním okně programu](#) na záložce **Aktualizace** klikněte na **Zkontrolovat aktualizace**.

3. Ručně, stažením instalačního balíčku z webových stránek společnosti ESET a [nainstalováním nejnovější verze](#) přes stávající.


Další informace a ilustrované návody:

- [Aktualizovat produkt ESET — zkontrolovat poslední moduly produktu](#)
- [Jaké typy produktových aktualizací ESET vydává?](#)

Automatická aktualizace starších produktů

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

[Známé problémy při instalaci](#)

 Každá nová verze produktu ESET opravuje chyby a vylepšuje funkce. Stávající zákazníci s platným předplatným produktu ESET mohou zdarma přejít na nejnovější verzi stejného produktu.

Pro dokončení instalace postupujte podle následujících kroků:

1. Klikněte na tlačítko **Přijmout a pokračovat** pro souhlas s [Licenčním ujednáním s koncovým uživatelem](#) a [Zásadami ochrany osobních údajů](#). Pokud nesouhlasíte s Licenčním ujednáním s koncovým uživatelem, klikněte na tlačítko **Odinstalovat**. Upozorňujeme, že tím ovšem není možný návrat k předešlé verzi produktu.
2. Klikněte na tlačítko **Přijmout vše a pokračovat** pro aktivování [systému zpětné vazby ESET LiveGrid®](#) a zapojení se do [Programu zvyšování spokojenosti zákazníků](#). Pokud se nechcete obou uvedených systémů účastnit, klikněte na tlačítko **Pokračovat**.
3. Po aktivaci nového produktu ESET pomocí aktivačního klíče se zobrazí stránka Přehled. Pokud nenaleznete informace o předplatném, použijte dál bezplatnou zkušební verzi. Pokud vaše předplatné použité u předchozího produktu není platné, [aktivujte produkt ESET](#).
4. Pro úplné dokončení instalace je vyžadován restart.

Nainstaluje se ESET Smart Security Premium

Toto dialogové okno se může zobrazit:

- Během instalačního procesu – pro instalaci klikněte na **Pokračovat**.
- Při změně předplatného v ESET Smart Security Premium – pro změnu předplatného a aktivaci ESET Smart Security Premium klikněte na **Aktivovat**.

V závislosti na vašem předplatném ESET můžete přepínat mezi domácími produkty ESET pro Windows pomocí možnosti **Změnit produkt**. Více informací naleznete v kapitole [Jaký mám produkt](#).

Přechod na jinou produktovou řadu

Podle svého předplatného ESET si můžete vybrat z produktů určených pro domácí uživatele na platformě Windows. Více informací naleznete v kapitole [Jaký mám produkt](#).

Registrace

Zaregistrujte si předplatné vyplněním polí v registračním formuláři a kliknutím na **Aktivovat**. Pole označená jako povinná je nutné vyplnit. Vámi poskytnuté informace budou použity pouze pro záležitosti týkající se vašeho předplatného ESET.

Průběh aktivace


Aktivační proces může chvíli trvat (v závislosti na rychlosti počítače a internetového připojení). Prosím, mějte strpení.

Úspěšná aktivace

Proces aktivace byl dokončen. Pro nastavení ESET Smart Security Premium postupujte podle kroků na obrazovce.

Do několika sekund se spustí aktualizace modulů. Následně se bude produkt ESET Smart Security Premium aktualizovat automaticky.


Do 20 minut od aktualizace modulů se spustí prvotní kontrola počítače.

 Proces aktivace může být přerušen, pokud nabídka není spojena s ESET HOME. Přihlaste se na ESET HOME nebo si vytvořte účet.

Jak začít

Tato kapitola poskytuje první seznámení s produktem ESET Smart Security Premium a jeho základním nastavením.

Ikona v oznamovací oblasti

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

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




Vypnout antivirovou a antispywarovou ochranu?

Vypnutím antivirové a antispywarové ochrany deaktivujete rezidentní ochranu souborového systému, ochranu přístupu na web, ochranu poštovních klientů a také Anti-Phishingovou ochranu. Tím vystavíte svůj počítač široké škále hrozeb.

Vypnout na 10 minut



 Použít

Zrušit

Dočasně vypnout firewall – přepne firewall do neaktivního režimu. Pro více informací přejděte do kapitoly [Sít'](#).

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

Rozšířená nastavení – otevře [Rozšířená nastavení](#) ESET Smart Security Premium. Pro otevření Rozšířených nastavení z [hlavního okna programu](#) stiskněte funkční klávesu F5 nebo klikněte na **Nastavení > Rozšířená**

nastavení.

[Protokoly](#) – protokoly obsahují informace o všech systémových událostech a poskytují přehled o nalezených hrozbách.

Otevřít ESET Smart Security Premium – otevře [hlavní okno programu](#) ESET Smart Security Premium.

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

Barevný režim – otevře rozšířené nastavení [Uživatelského rozhraní](#), kde můžete změnit barvu grafického rozhraní.

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

[O programu](#) – poskytuje informace o instalovaném programu ESET Smart Security Premium a všech jeho programovaných modulech. Také zde naleznete informace o operačním systému a systémových prostředcích.

Klávesové zkratky

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

Klávesové zkratky	Akce
F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Šipka nahoru / šipka dolů	přesun v položkách rozbalovací nabídky
TAB	přesun na následující ovládací prvek v uživatelském rozhraní
Shift+TAB	přesun na předchozí ovládací prvek v uživatelském rozhraní
ESC	zavře zobrazené dialogové okno
Ctrl+U	zobrazí informace o vašem předplatném ESET a vašem počítači (podrobnosti pro technickou podporu)
Ctrl+R	obnoví pozici a velikost okna na výchozí hodnoty
ALT + šipka vlevo	přesun zpět
ALT + šipka vpravo	přesun vpřed
ALT+Home	přesun na úvodní obrazovku

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

Profily

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

Kontrola počítače

K dispozici jsou čtyři předdefinované profily kontroly ESET Smart Security Premium:

- **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.
- **Hlubková kontrola počítače:** Profil hloubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.
- **Kontrola počítače:** Toto je výchozí profil používaný při standardní kontrole počítače.

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

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

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

Aktualizace

Editor profilů v [Nastavení aktualizace](#) umožňuje vytvářet nové aktualizací profily. Ty se používají pouze v případě, že používáte různé způsoby připojení na aktualizací 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 aktualizací profilů.

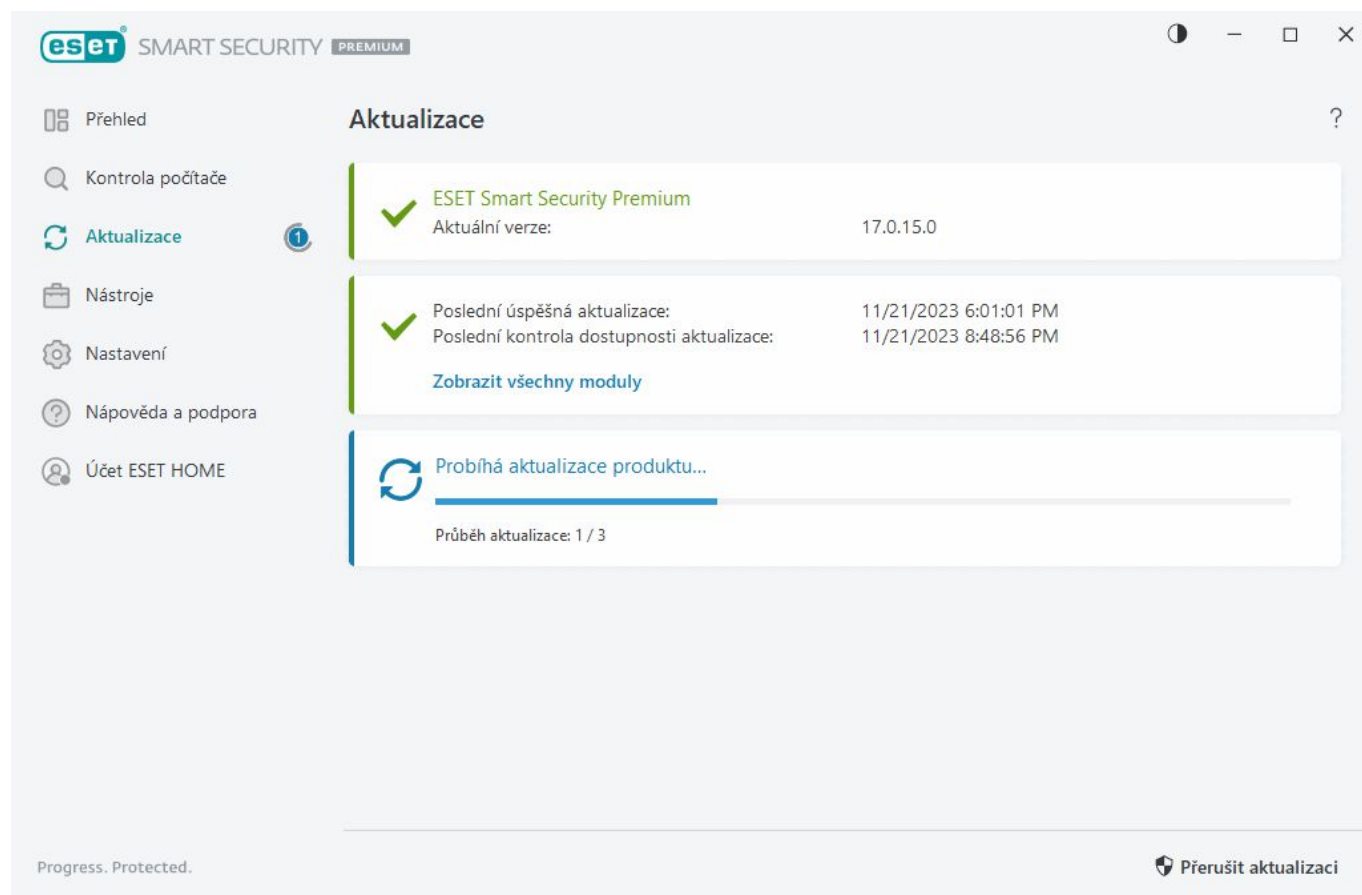
Aktualizace

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

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

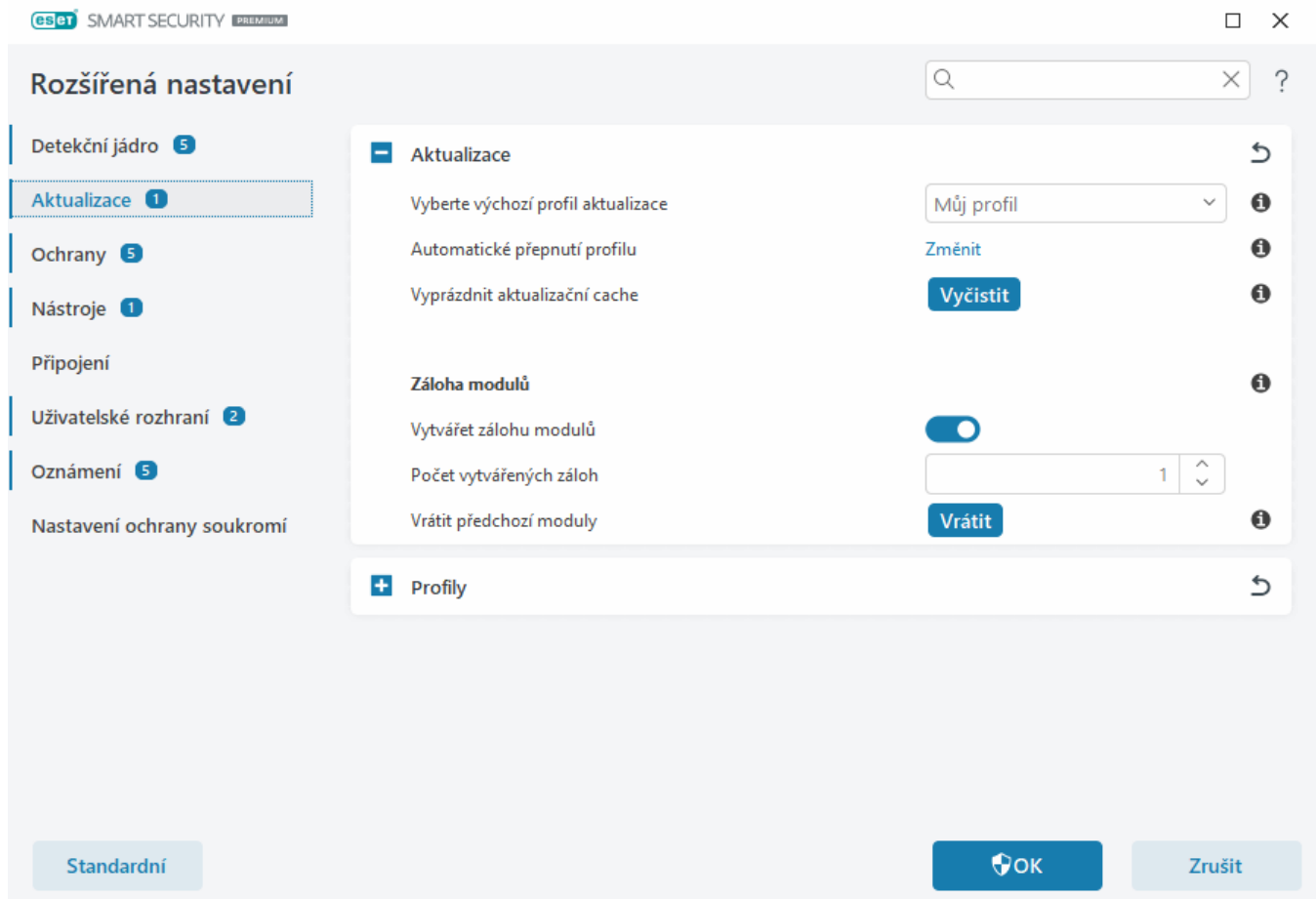
Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na

tlačítko **Zkontrolovat aktualizace**.



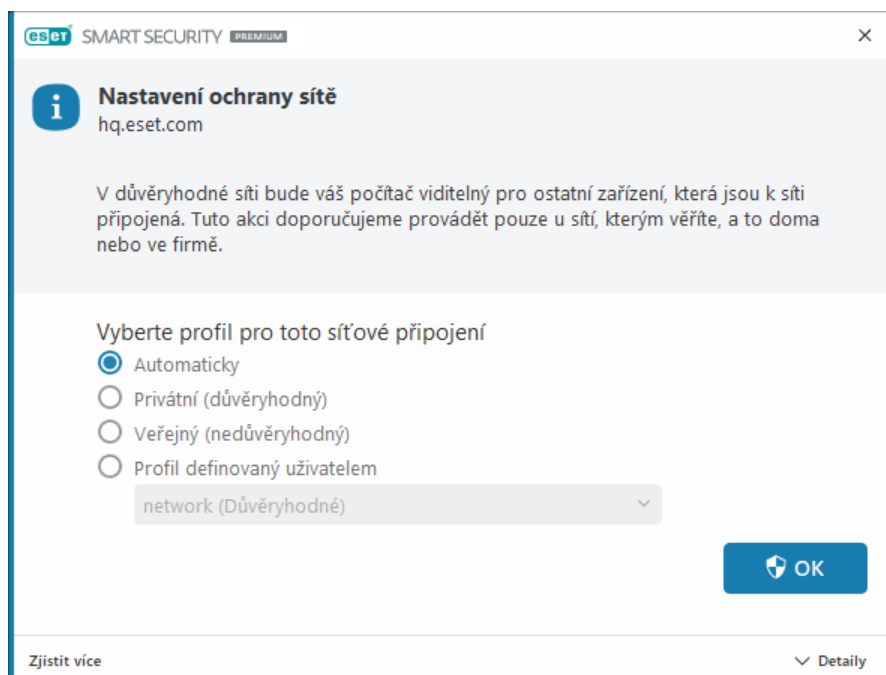
V [Rozšířených nastaveních](#) > **Aktualizace** najdete další možnosti, například režim aktualizace, přístup k proxy serveru a připojení k síti LAN.

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



Nastavení ochrany sítě

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




Můžete si vybrat z následujících [profilů síťových připojení](#):

Automaticky – ESET Smart Security Premium vybere profil automaticky na základě [Spouštěčů](#) nakonfigurovaných pro každý profil.

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

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

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


 Nesprávným nastavením sítě může být počítač ohrožen.

Aktivace Anti-Theft


Osobní zařízení jsou neustále vystavena riziku ztráty nebo krádeže během našich každodenních cest z domova do práce nebo na jiná veřejná místa. Anti-Theft je funkce, která rozšiřuje zabezpečení uživatele v případě ztráty nebo krádeže zařízení. Anti-Theft umožňuje sledovat používání zařízení a dohledat ztracené zařízení pomocí lokalizace podle IP adresy ve [ESET HOME](#), čímž vám pomůže získat zařízení zpět a ochránit osobní údaje.

Pomocí moderních technologií, jako je vyhledávání zařízení podle IP adresy, vzdálená aktivace webové kamery nebo uzamknutí uživatelských účtů, Anti-Theft ochrání data uložená ve vašem počítači či jiném zařízení v případě jeho ztráty nebo odcizení a zároveň vám pomůže zjistit jeho polohu. Stejně tak následně na [ESET HOME](#) můžete sledovat aktivity na vašem počítači nebo mobilním zařízení pohodlně prostřednictvím internetového prohlížeče nebo mobilní aplikace.

Více informací týkající se technologie Anti-Theft naleznete v [online příručce k portálu ESET HOME](#).

 Anti-Theft nemusí správně fungovat u počítačů připojených do domény kvůli omezením ve správě uživatelských účtů.

Pro zapnutí technologie Anti-Theft a ochranu dat uložených v zařízení v případě jeho ztráty nebo odcizení si vyberte jeden z níže uvedených postupů:

- V [hlavním okně programu](#) v části **Přehled** klikněte na **NASTAVIT** vedle položky **Anti-Theft**.
- Pokud se v [hlavním okně programu](#) zobrazuje sdělení "Anti-Theft je dostupný", klikněte na záložce **Přehled** na možnost **Zapnout Anti-Theft**.
- V [hlavním okně programu](#) přejděte na záložku **Nastavení** > **Bezpečnostní nástroje**. Přepínačem aktivujte  **Anti-Theft** a postupujte podle pokynů na obrazovce.

Pokud není vaše zařízení [připojeno k účtu ESET HOME](#):

1. Pro zapnutí funkce Anti-Theft se [Přihlaste ke svému účtu ESET HOME](#).
2. [Zadejte název zařízení](#).

i Anti-Theft nepodporuje Microsoft Windows Home Server.

Po zapnutí funkce Anti-Theft si [nastavte způsob zabezpečení svého zařízení](#) v [hlavním okně programu](#) > **Nastavení** > **Bezpečnostní nástroje** > **Anti-Theft**.

Rodičovská kontrola

Pokud jste zapnuli [Rodičovskou kontrolu](#) v ESET Smart Security Premium, nastavte také konkrétní uživatelské účty, kterých se rodičovská kontrola týká.

Pokud je Rodičovská kontrola zapnutá, ale žádný účet nebyl nastaven, v hlavním okně programu se v části **Přehled** zobrazí informace Rodičovská kontrola není nastavena. Klikněte na položku **Nastavit pravidla** viz [kapitola Rodičovská kontrola](#).

Aktivace produktu

Produkt můžete aktivovat několika způsoby. Dostupnost jednotlivých metod závisí na zemi a způsobu distribuce (CD/DVD, webové stránky společnosti ESET, apod.):

- Pokud jste si zakoupili krabicovou verzi produktu nebo jste obdrželi e-mail s údaji o předplatném, aktivujte produkt kliknutím na možnost **Použít zakoupený aktivační klíč**. Pro úspěšnou aktivaci je nutné zadat aktivační klíč tak, jak jste jej obdrželi. Aktivační klíč je jedinečný řetězec ve formátu XXXX-XXXX-XXXX-XXXX-XXXX nebo XXXX-XXXXXX, který slouží k identifikaci vlastníka předplatného a k aktivaci. Aktivační klíč se obvykle nachází uvnitř nebo na zadní straně krabice.
- Po vybrání možnosti [Použít účet ESET HOME](#) budete vyzváni k zadání přihlašovacích údajů ke svému účtu ESET HOME.
- Pokud si chcete produkt ESET Smart Security Premium nejprve vyzkoušet, vyberte možnost [Zkušební verze](#). Následně budete vyzváni k výběru země a zadání e-mailové adresy, ke které budete mít zkušební verzi ESET Smart Security Premium vázanou. Bezplatná zkušební verze vám bude zaslána e-mailem. Bezplatnou zkušební verzi může zákazník aktivovat pouze jednou.
- Pokud nemáte předplatné a chcete si ho zakoupit, klikněte na **Zakoupit předplatné**. Následně budete přesměrováni na webové stránky lokálního distributora ESET. Předplatné produktu ESET pro domácnosti na platformě Windows [není zdarma](#).

Předplatné produktu můžete kdykoli změnit. Stačí kliknout v [hlavním okně programu](#) na **Nápověda a podpora** > **Změnit předplatné**. Zobrazí se veřejné ID, které slouží k identifikaci vašeho předplatného při komunikaci s technickou podporou společnosti ESET.

! [Neúspěšná aktivace?](#)

Vyberte si způsob aktivace



Použít účet ESET HOME

Přihlaste se ke svému účtu ESET HOME a vyberte licenci, kterou chcete aktivovat produkt ESET na tomto zařízení.



Použít zakoupený licenční klíč

Použijte licenci, kterou jste si zakoupili online nebo v kamenném obchodě.



Objednat licenci

Pro zakoupení nové licence kontaktujte svého lokálního prodejce. Pokud si nejste jisti, kdo je náš prodejce ve vašem okolí, [kontaktujte naši podporu](#).

Zadání aktivačního klíče během aktivace

Pro správný chod bezpečnostního produktu ESET Smart Security Premium je důležité, aby byl automaticky aktualizován.

Při zadávání **aktivačního klíče** je důležité, abyste jej zadali přesně. Váš aktivační klíč je jedinečný řetězec ve formátu XXXX-XXXX-XXXX-XXXX-XXXX který se používá k identifikaci vlastníka předplatného a k aktivaci předplatného.

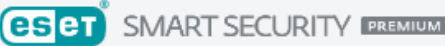
Doporučujeme zkopírovat a vložit aktivační klíč z registračního e-mailu, aby byla zajištěna jeho správnost.

Pokud po instalaci ne zadáte aktivační klíč, produkt nebude aktivován. ESET Smart Security Premium můžete aktivovat v [hlavním okně programu](#) > **Nápověda a podpora** > **Aktivovat předplatné**.


Předplatná pro produkty ESET pro domácnosti na platformě Windows [nejsou zdarma](#).


Použití účtu ESET HOME


Pro zobrazení a správu předplatného, včetně aktivovaných zařízení, připojte zařízení k [ESET HOME](#). Můžete zobrazit důležité podrobnosti o předplatném, obnovit jej, prodloužit nebo přejít na vyšší úroveň předplatného. Na portálu ESET HOME nebo v mobilní aplikaci můžete přidávat různá předplatná, stahovat produkty do svých zařízení, kontrolovat stav jejich zabezpečení nebo sdílet předplatné prostřednictvím e-mailu. Více informací naleznete v [Online nápovědě ESET HOME](#).





Přihlášení k účtu ESET HOME

 Přihlásit se pomocí Google

 Přihlásit se pomocí Apple

 Naskenovat QR kód






E-mailová adresa

Heslo

[Zapomněli jste heslo?](#)

 Přihlásit se

Zrušit

Nemáte účet? [Vytvořte si jej!](#)

Po výběru **Použít účet ESET HOME** jako aktivační metody nebo při připojení k účtu ESET HOME během instalace:

1. [Přihlaste se ke svému účtu ESET HOME.](#)



Pokud zatím nemáte účet ESET HOME, pro registraci nebo zobrazení instrukcí v [Online nápovědě ESET HOME](#) klikněte na tlačítko **Vytvořit účet**.

V případě, že si na heslo nemůžete vzpomenout, klikněte na možnost **Zapomněli jste heslo?** a pokračujte dle instrukcí v [Online nápovědě ESET HOME](#).

2. Zadejte **Název zařízení**, pod kterým bude zobrazené v portálu ESET HOME a klikněte na možnost **Pokračovat**.
3. Vyberte předplatné k aktivaci nebo [přidejte nové předplatné](#). Klikněte na tlačítko **Pokračovat** a dokončete aktivaci produktu ESET Smart Security Premium.

Aktivovat zkušební verzi

Pro aktivaci zkušební licence ESET Smart Security Premium zadejte platnou adresu do pole **E-mailová adresa** a **Potvrdit e-mailovou adresu**. Po aktivaci bude vygenerováno předplatné ESET a zasláno na váš e-mail. Adresa bude také použita pro oznámení před ukončením platnosti licence a pro další komunikaci se společností ESET. Bezplatnou zkušební verzi lze aktivovat pouze jednou.

Z rozbalovacího menu **Země** vyberte zemi pro registraci produktu ESET Smart Security Premium u lokálního distributora, který vám bude poskytovat technickou podporu.

Bezplatný aktivační klíč ESET

Předplatné pro ESET Smart Security Premium není zdarma.

Aktivační klíč ESET je unikátní sekvence písmen a čísel oddělených pomlčkou, kterou poskytuje společnost ESET, aby umožnila legální používání ESET Smart Security Premium v souladu s [Licenčním ujednáním s koncovým uživatelem](#). Každý koncový uživatel je oprávněn používat aktivační klíč pouze v rozsahu, v jakém má právo používat ESET Smart Security Premium na základě počtu licencí udělených společnostmi ESET. Aktivační klíč je důvěrný a nelze jej sdílet. Můžete však [sdílet předplatné pomocí ESET HOME](#).

Na internetu můžete nalézt velké množství webových stránek, které vám mohou nabízet aktivační klíč ESET "zdarma", ale pamatujte:

- Kliknutím na reklamu „předplatné ESET zdarma“ může dojít ke kompromitaci vašeho počítače nebo zařízení a riskujete jeho napadení škodlivým kódem. Malware se může šířit prostřednictvím neoficiálního obsahu internetu (např. z různých fór nebo videí), z webových stránek slibujících zisk finančního obnosu na základě jejich navštívení apod. Jsou to běžné postupy, jak obelhat uživatele.
- Společnost ESET může zakázat pirátské předplatné a také to dělá.
- Aktivace produktu pomocí pirátského aktivačního klíče není v souladu s [Licenčním ujednáním s koncovým uživatelem](#), které přijímáte instalací ESET Smart Security Premium.
- Předplatné na produkty ESET kupujte výhradně prostřednictvím oficiálních kanálů, například na webových stránkách www.eset.com, u distributorů a prodejců ESET. Nikdy nenakupujte předplatné na neoficiálních webových stránkách, jako je eBay, nebo sdílené předplatné poskytnuté třetí stranou.
- [Stažení](#) ESET Smart Security Premium je bezplatné, ovšem v průběhu instalace je vyžadována aktivace platným aktivačním klíčem (produkt si můžete stáhnout a nainstalovat, ale bez aktivace nebude fungovat).
- Nesdílejte nikdy své předplatné na internetu nebo sociálních médiích (mohlo by dojít k jeho zneužití).

Jak rozpoznat pirátské předplatné ESET, a jak jej nahlásit, se dovíte v [Databázi znalostí](#).

Pokud jste se dosud nerozhodli k zakoupení bezpečnostního produktu ESET, můžete zatím využít zkušební verzi:

1. [Aktivujte ESET Smart Security Premium bezplatnou zkušební verzí](#)
2. [Zapojte se do ESET Beta programu](#)
3. Pokud používáte zařízení s operačním systémem Android, [nainstalujte si ESET Mobile Security](#). Jedná se o freemium.

Chcete-li získat slevu nebo prodloužit předplatné, [obnovte své předplatné ESET](#).

Neúspěšná aktivace – běžné scénáře

Nejčastější problémy s aktivací ESET Smart Security Premium mohou být:

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

Zkontrolujte, zda jste zadali správný aktivační klíč a zda je vaše internetové připojení aktivní. Zkuste aktivovat ESET Smart Security Premium znovu. Jestliže pro aktivaci používáte účet ESET HOME, přečtěte si kapitolu Online nápovědy věnovanou [předplatnému a správě předplatného pro ESET HOME](#).

i Pokud se zobrazí určitá chyba (například Pozastavené předplatné nebo Nadužívané předplatné), postupujte podle pokynů v sekci [Stav předplatného](#).

Pokud se vám stále nedaří produkt ESET Smart Security Premium aktivovat, náš [ESET průvodce aktivací](#) vám poskytne odpovědi na nejčastější dotazy, aktivační chyby a problémy společně s informacemi týkajícími se licencování produktu.

Stav předplatného

Vaše předplatné může být různém stavu. Informaci o stavu svého předplatného najdete v [ESET HOME](#). Chcete-li přidat předplatné ke svému účtu ESET HOME, podívejte se do článku [o přidávání předplatného](#).

i Pokud ještě účet ESET HOME nemáte, přečtěte si rovněž [Vytvoření nového účtu ESET HOME](#).

Pokud je stav předplatného jiný než **Aktivní**, zobrazí se při aktivaci chyba nebo oznámení v [hlavním okně programu](#).

Chcete-li zakázat oznámení o stavu předplatného, otevřete [Rozšířená nastavení](#) > **Oznámení** > **Stavy aplikací**. Následně klikněte na **Změnit**, rozbalte seznam **Licencování** a odklikněte pole v řádku oznámení, které chcete vypnout. Vypnutí oznámení problém nevyřeší.

Popisy a doporučená řešení pro různé stavy předplatného naleznete v tabulce níže:

Stav předplatného	Popis	Řešení
Aktivní	Předplatné je platné a není nutná vaše interakce. ESET Smart Security Premium lze aktivovat a podrobnosti o předplatném najdete v hlavním okně programu > Nápověda a podpora .	
Nadužívané	Toto předplatné používá více zařízení, než je povoleno. Zobrazí se chyba aktivace.	Další informace naleznete v kapitole Aktivace se nezdařila z důvodu nadužívání předplatného .

Stav předplatného	Popis	Řešení
Pozastaveno	Vaše předplatné bylo pozastaveno z důvodu problémů s platbou. Chcete-li předplatné používat, ujistěte se, že jsou vaše platební údaje na ESET HOME aktuální , nebo se obraťte na prodejce předplatného. Oznámení o této chybě se vám zobrazí během aktivace produktu nebo v hlavním okně programu .	Nainstalovaný produkt – pokud máte účet ESET HOME, klikněte v oznámení zobrazeném v hlavním okně programu na možnost Spravujte své předplatné v ESET HOME a zkontrolujte své platební údaje . V opačném případě kontaktujte prodejce předplatného. Chyba při aktivaci – pokud máte účet ESET HOME, v okně s oznámením o chybě při aktivaci klikněte na Přejít na ESET HOME a zkontrolujte své platební údaje . V opačném případě kontaktujte prodejce předplatného.
Vypršelo	Platnost vašeho předplatného vypršela a toto předplatné nemůžete použít k aktivaci ESET Smart Security Premium. Oznámení o této chybě se vám zobrazí během aktivace produktu nebo v hlavním okně programu . Pokud již nainstalovali ESET Smart Security Premium, vaše zařízení není chráněno a aktualizováno.	Nainstalovaný produkt – v oznámení zobrazeném v hlavním okně programu klikněte na Obnovit předplatné a postupujte podle pokynů v kapitole Jak obnovit předplatné? nebo klikněte na Aktivovat produkt a vyberte způsob aktivace . Chyba při aktivaci – v okně s oznámením o chybě při aktivaci klikněte na Obnovit předplatné a postupujte podle pokynů v kapitole Jak obnovit předplatné? nebo zadejte nový nebo obnovený aktivační klíč a klikněte na Obnovit předplatné .
Zrušeno	Vaše předplatné bylo zrušeno společností ESET nebo prodejcem předplatného.	Pokud se zobrazí chyba: Předplatné bylo zrušeno v hlavním okně programu nebo během aktivace (a předplatné by mělo fungovat správně), kontaktujte prodejce předplatného.

Neúspěšná aktivace z důvodu nadužívání předplatného

Problém

- Vaše předplatné může být nadměrně využíváno nebo zneužíváno
- Neúspěšná aktivace z důvodu nadužívání předplatného

Řešení

Tato předplatné je používáno na více zařízeních, než je povoleno. Pravděpodobně jste se stali obětí softwarového pirátství nebo padělání. Předplatné nelze použít k aktivaci žádného dalšího produktu ESET. Tento problém můžete vyřešit přímo, pokud jste oprávněni ke správě předplatného pomocí účtu ESET HOME nebo jste si předplatné zakoupili z legitimního zdroje. Pokud ještě nemáte účet, vytvořte si jej.

Pokud jste vlastníky předplatného a nebyli jste vyzváni k zadání e-mailové adresy:

1. Pro správu předplatného ESET otevřete webový prohlížeč a přejděte na stránku <https://home.eset.com>. Přejděte do sekce ESET License Manager, kde odstraňte již nepoužívaná zařízení, případně licenci deaktivujte na zařízeních, na kterých ji nechcete používat. Pro více informací si přečtěte článek [Co dělat v případě, že je předplatné nadužíváno](#).
2. Jak identifikovat a nahlásit pirátské předplatné ESET se dozvíte v článku v [Databázi znalostí](#), kde naleznete pokyny.
3. Pokud si nejste jisti, klikněte na tlačítko **Zpět** a použijte odkaz [Technická podpora společnosti ESET](#).

Pokud nejste vlastníkem předplatného, kontaktujte vlastníka tohoto předplatného a informujte jej, že nemůžete aktivovat produkt ESET z důvodu nadužívání předplatného. Vlastník může vyřešit problém na portále [ESET HOME](#).

Pokud jste požádáni o potvrzení e-mailové adresy (pouze v některých případech), zadejte tu, kterou jste použili při nákupu a aktivaci ESET Smart Security Premium.

Práce s ESET Smart Security Premium

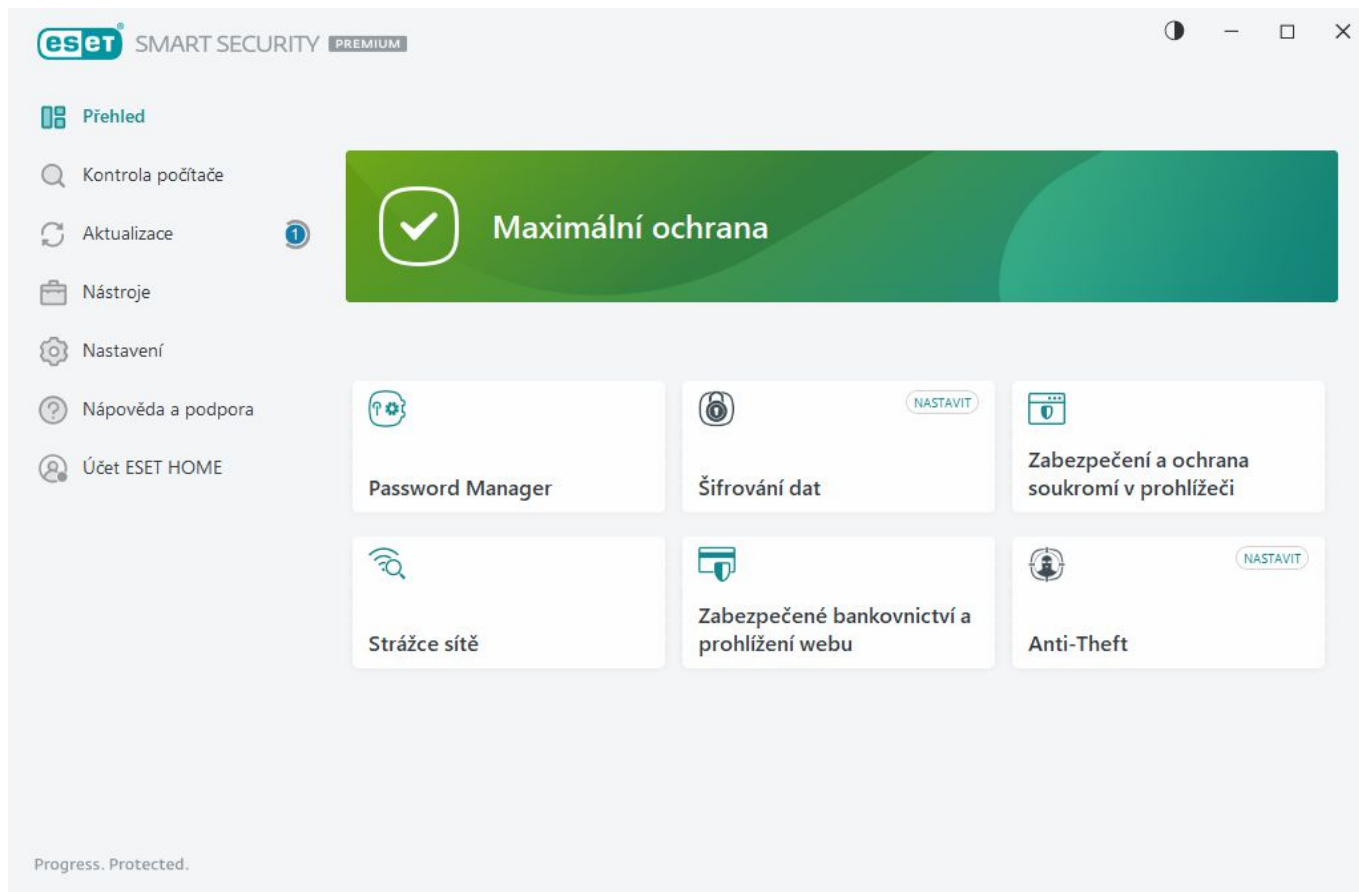
Hlavní okno programu ESET Smart Security Premium je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Názorné ukázky

- i** Názorné ukázky, jak otevřít hlavní okno produktu, máme k dispozici v [Databázi znalostí](#) v angličtině a několika dalších jazycích.

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

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



Položky hlavního menu:

[Přehled](#) – poskytuje informace o událostech a stavu ochrany ESET Smart Security Premium.

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

[Aktualizace](#) – zobrazuje informace o aktualizacích detekčního jádra a programových modulů.

[Nástroje](#) – umožňují nastavit [Strážce sítě](#) a další funkce, které pomáhají zjednodušit správu programu a nabízejí další možnosti pro pokročilé uživatele.

[Nastavení](#) – umožňují konfiguraci bezpečnostních funkcí ESET Smart Security Premium (Ochrana počítače, Internetová ochrana, Síťová ochrana a Bezpečnostní nástroje) a přístup k [Rozšířeným nastavením](#).

[Návod a podpora](#) – zobrazuje informace o vašem předplatném, nainstalovaném produktu ESET a odkazy na [Online nápovědu](#), [Databázi znalostí](#) a [Technickou podporu](#).

[Účet ESET HOME](#) – v této části můžete [připojit zařízení ke svému účtu ESET HOME](#) nebo zkontrolovat stav připojení k účtu. Použijte [ESET HOME](#) pro zobrazení a správu nastavení Anti-Theft a aktivovaného předplatného ESET a zařízení.

Přehled


V části **Přehled** se zobrazují informace o aktuální ochraně počítače spolu s rychlými odkazy na bezpečnostní funkce ESET Smart Security Premium.

V okně **Přehled** se zobrazují [oznámení](#) s podrobnými informacemi a doporučenými řešeními událostí v ESET Smart

Security Premium, pro zapnutí dalších funkcí nebo zajištění maximální ochrany. Pokud je oznámení více, kliknutím na **více oznámení** je všechny rozbalíte.

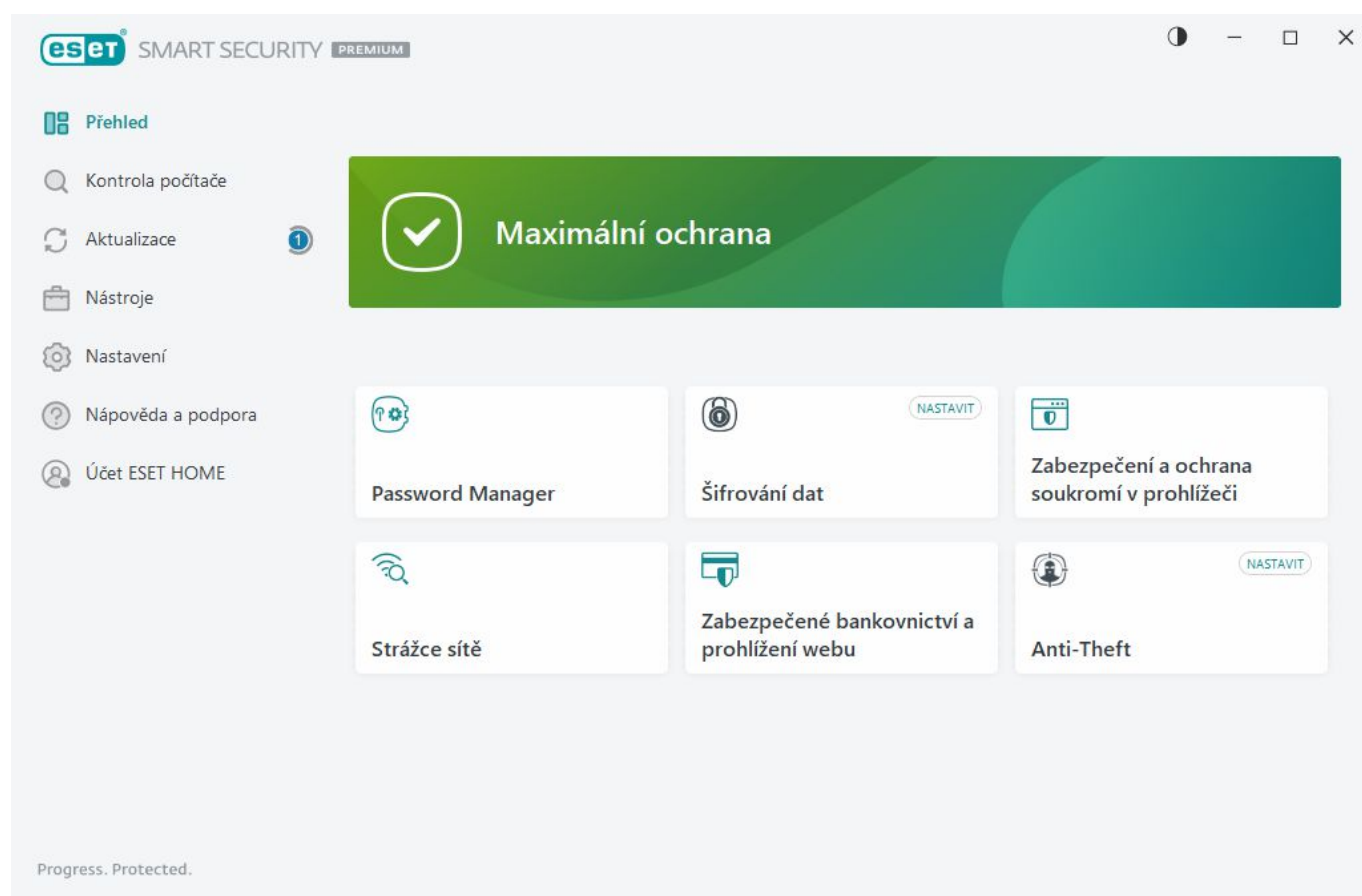
Password Manager – otevírá pokyny k nastavení [Password Manager](#).

Strážce sítě – kontroluje zabezpečení vaší sítě.

Secure Data – otevře sekci [Bezpečnostní nástroje](#). Klikněte na přepínač  vedle položky **Secure Data** a aktivujte ji. Pokud již máte nastavenou službu Secure Data, otevře se přímo sekce [Secure Data](#).

Zabezpečené bankovníctví a prohlížení webu – v zabezpečeném režimu spustí prohlížeč, který je ve Windows nastavený jako výchozí.

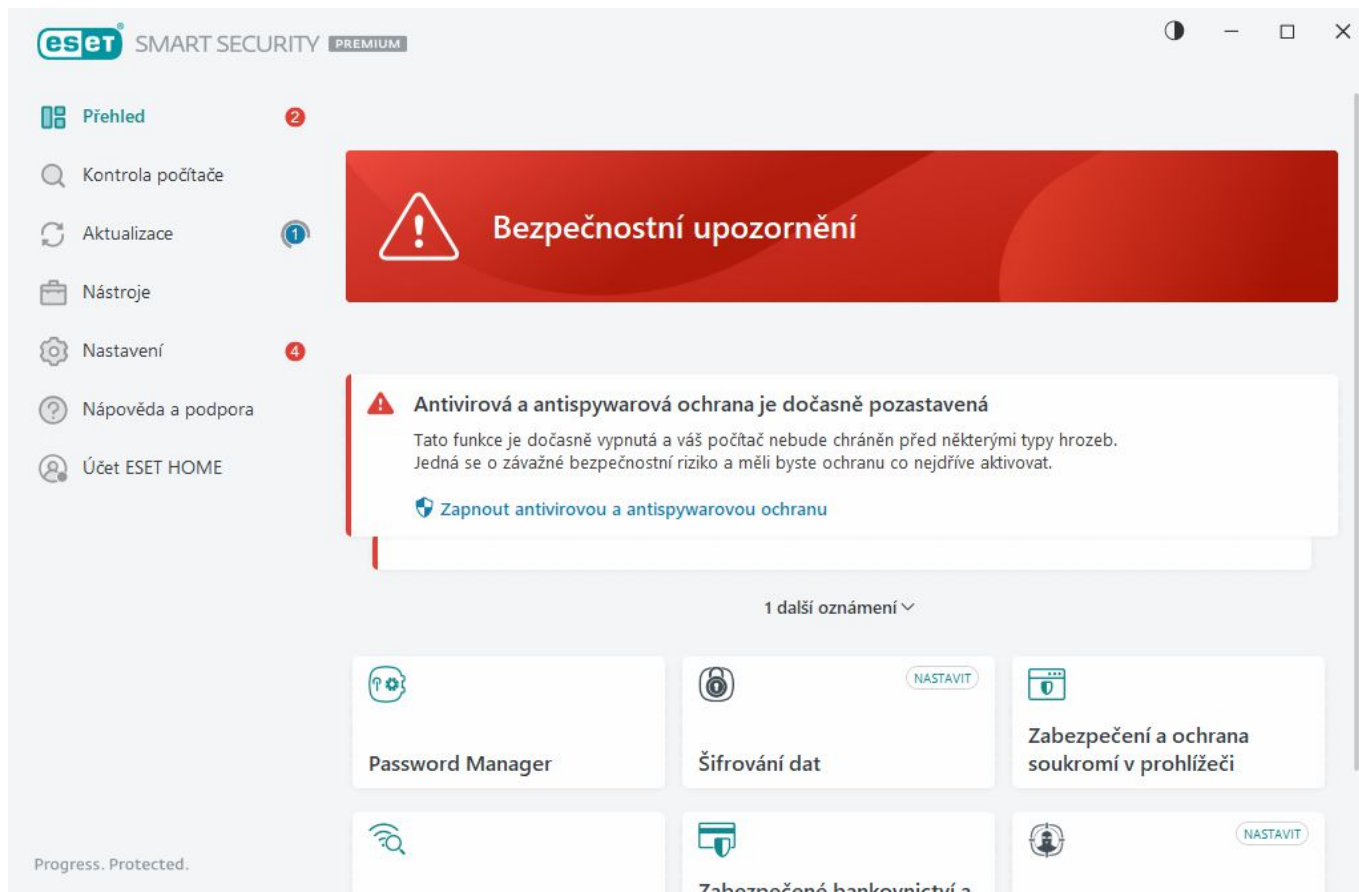
Anti-Theft – spustí [nastavení služby Anti-Theft](#). Pokud již máte nastavenou službu Anti-Theft, otevře se přímo sekce [Anti-Theft](#).



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

Co dělat, když program nepracuje správně?

Při plné funkčnosti ochrany má ikona **Stavu ochrany** zelenou barvu. V opačném případě je barva stavu ochrany červená nebo žlutá a zobrazuje se informace, že není zajištěna maximální ochrana. Zároveň jsou na záložce **Přehled** zobrazeny [bližší informace](#) o stavu jednotlivých modulů a návrh na možné řešení problému pro obnovení maximální ochrany. Stav jednotlivých modulů můžete změnit kliknutím na záložku **Nastavení** a vybráním požadovaného modulu.



Červená ikona a červené **bezpečnostní upozornění** signalizují kritické problémy.

Ochrana vašeho systému není zajištěna v plné míře. Možné příčiny jsou:

- **Produkt není aktivován** nebo **Předplatné vypršelo** – ikona stavu ochrany je červená. Po vypršení předplatného není možné program aktualizovat. Obnovte své předplatné podle pokynů v okně s upozorněním.
- **Detekční jádro není aktuální** – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci detekčního jádra. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Mezi nejčastější důvody patří nesprávně zadaná [ověřovací data](#) nebo nesprávně nastavené [připojení k internetu](#).
- **Rezidentní ochrana souborového systému je dočasně vypnutá** – rezidentní ochrana byla vypnuta uživatelem. Váš počítač není chráněn před hrozbami. Pro opětovné zapnutí Rezidentní ochrany souborového systému klikněte na **Zapnout rezidentní ochranu**.
- **Antivirová a antispywarová ochrana je vypnutá** – ochranu zapněte kliknutím na **Zapnout antivirovou a antispywarovou ochranu**.
- **Firewall je dočasně vypnutý** – na problém budete upozorněni bezpečnostním oznámením v hlavním okně programu. Znovu zapnout síťovou ochranu můžete kliknutím na **Zapnout firewall**.



Oranžová ikona signalizuje omezenou ochranu. Může se například vyskytnout problém s aktualizací programu nebo se blíží konec platnosti vašeho předplatného.

Tento stav se může zobrazit z několika důvodů, například:

- **Nedostatečná nastavení zařízení pro službu Anti-Theft** – toto zařízení není optimalizované pro využití služby Anti-Theft. Fantom účet (bezpečnostní řešení spouštěné automaticky v případě označení zařízení za ztracené) nemůže být vytvořen. Fantom účet vytvoříte ve webovém rozhraní Anti-Theft v

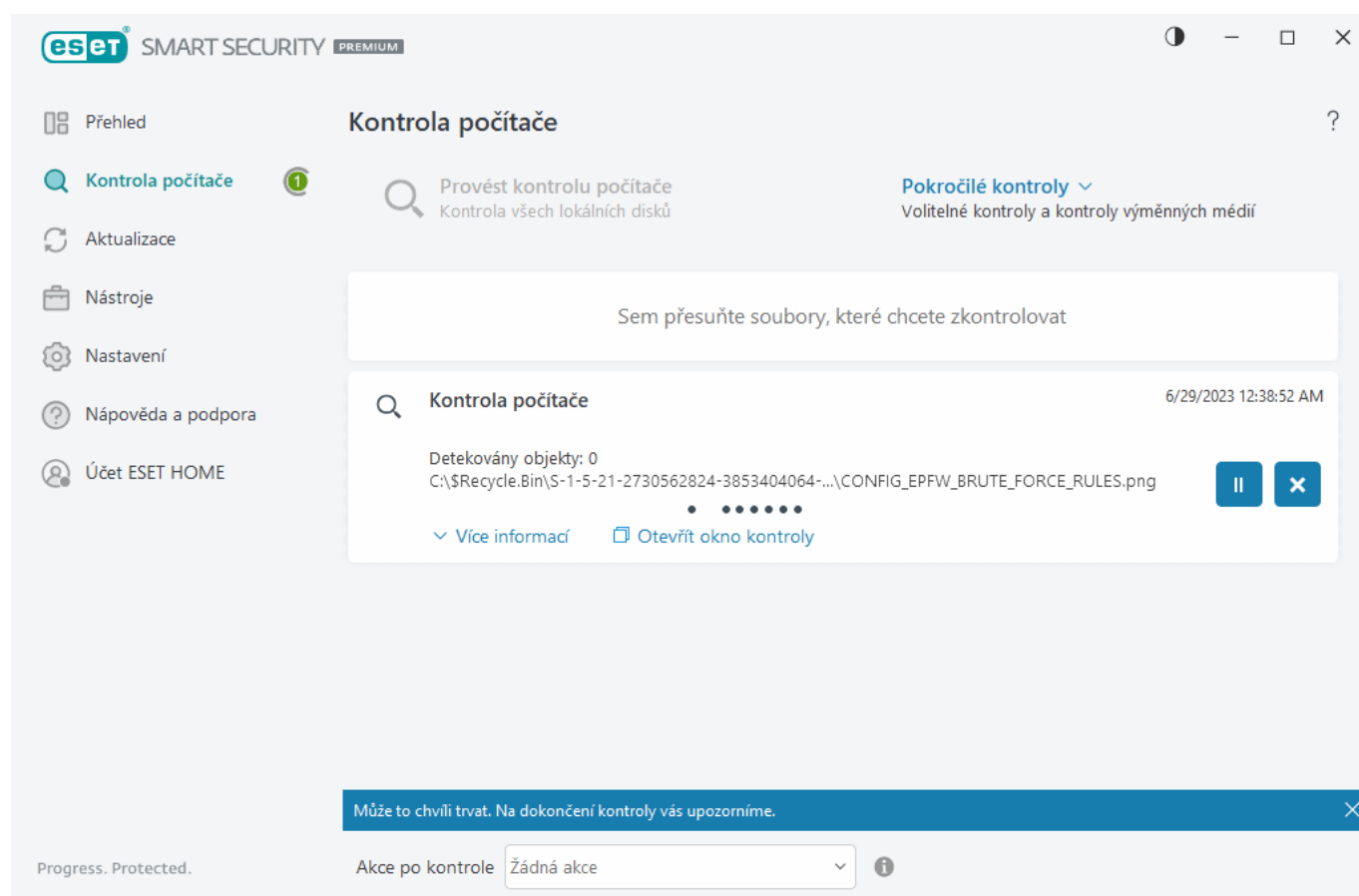
části [Nastavení](#).

- **Herní režim je zapnutý** – zapnutí [Herního režimu](#) představuje potenciální bezpečnostní riziko. Povolením této funkce zakážete všechna okna s oznámeními nebo upozorněními a zastavíte všechny naplánované úlohy.
- **Blíží se konec platnosti předplatného / Platnost vašeho předplatného dnes vyprší** – to je indikováno ikonou stavu ochrany zobrazující vykřičník vedle systémových hodin. Po vypršení platnosti předplatného nebude možné program aktualizovat a ikona stavu ochrany změní barvu na červenou.

V případě, že není možné problém vyřešit, 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, pošlete dotaz na technickou podporu. Specialisté technické podpory ESET vám odpoví v co nejkratším možném čase a pomohou vám s řešením problému.

Kontrola počítače

Důležitou součástí antivirového řešení 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. Hlubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech, aby byl detekován případný malware, který v době zápisu na disk nebyl zachycen [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 vir.



K dispozici jsou dva typy **kontroly počítače**. Pokud kliknete na možnost **Provést kontrolu počítače**, spustí se rychlá kontrola systému bez nutnosti specifikovat parametry kontroly. **Volitelná kontrola** (po kliknutí na Pokročilé

kontroly), umožňuje vybrat předdefinované profily kontroly, které jsou navrženy tak, aby cílily na konkrétní místa a také vybraly konkrétní cíle kontroly.

Více informací o procesu kontroly naleznete v kapitole [Průběh kontroly](#).

i Ve výchozím stavu se ESET Smart Security Premium pokusí automaticky vyléčit nebo smazat objekty, které detekoval během kontroly počítače. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Instrukce pro změnu úrovně léčení společně s jejich detailním popisem máme uveden v kapitole [Úroveň léčení](#). Výsledky provedených kontrol naleznete v [Protokolech](#).

Provést kontrolu počítače

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

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

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

Volitelná kontrola

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

Kontrola výměnných médií

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

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

Opakovat poslední kontrolu

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

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

- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.
- **Vypnout** – počítač se po dokončení kontroly vypne,
- **Restartovat v případě potřeby** – počítač se po dokončení kontroly restartuje, pokud je to potřeba pro

dokončení léčení detekovaných hrozeb.

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

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

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

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

Spuštění volitelné kontroly

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

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

Další cíle kontroly si můžete vybrat ve stromové struktuře.

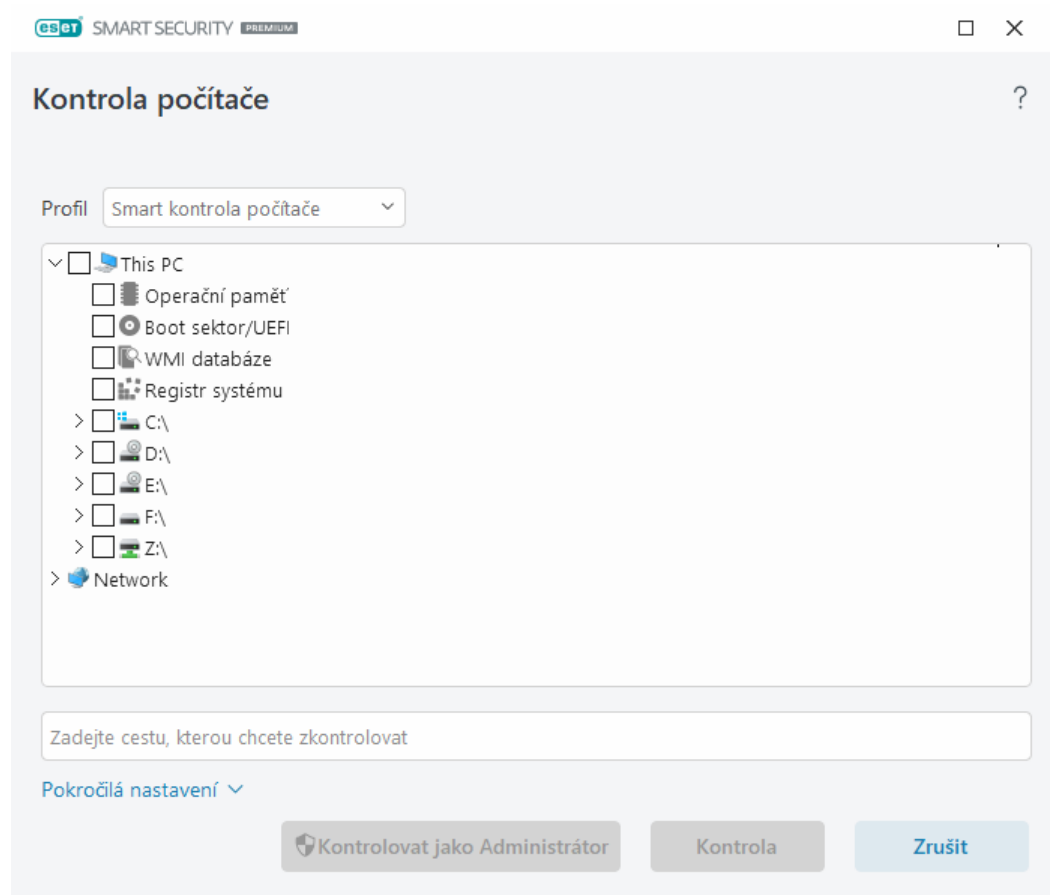
- **Operační paměť** – kontrola všech procesů a dat aktuálně nahranych v operační paměti.
- **Boot sektory/UEFI** – kontrola přítomnosti škodlivého kódu v boot sektorech disků a UEFI. Pro více informací o UEFI skeneru přejděte do [slovníku pojmů](#).
- **WMI databáze** – kontrola celé Windows Management 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 zaškrtnutí pole ve stromové struktuře přidáte daný cíl do seznamu cílů, které se mají kontrolovat.

i Jak naplánovat každý týden kontrolu počítače?
Přečtěte si kapitolu [Jak naplánovat kontrolu počítače jednou týdně?](#).



Parametry léčení použité v daném profilu kontroly můžete změnit v [Rozšířených nastaveních](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola** > **ThreatSense** > **Léčení**. V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, klikněte na **Rozšířená nastavení** a následně vyberte možnost **Neléčit**. Historie kontrol je zaznamenána do protokolu kontrol.

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

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

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

i Protokol kontroly po jejím ukončení zobrazíte kliknutím na tlačítko [Zobrazit protokol](#).

Průběh kontroly

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



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



Jak naplánovat každý týden kontrolu počítače?

Přečtěte si kapitolu [Jak naplánovat kontrolu počítače jednou týdně?](#).

Průběh kontroly – ukazatel průběhu zobrazuje stav probíhající kontroly.

Cíl – název právě kontrolovaného souboru a jeho umístění.

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

Kliknutím na Více informací se zobrazí následující informace:

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

Ikona pozastavení – přeruší kontrolu.

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

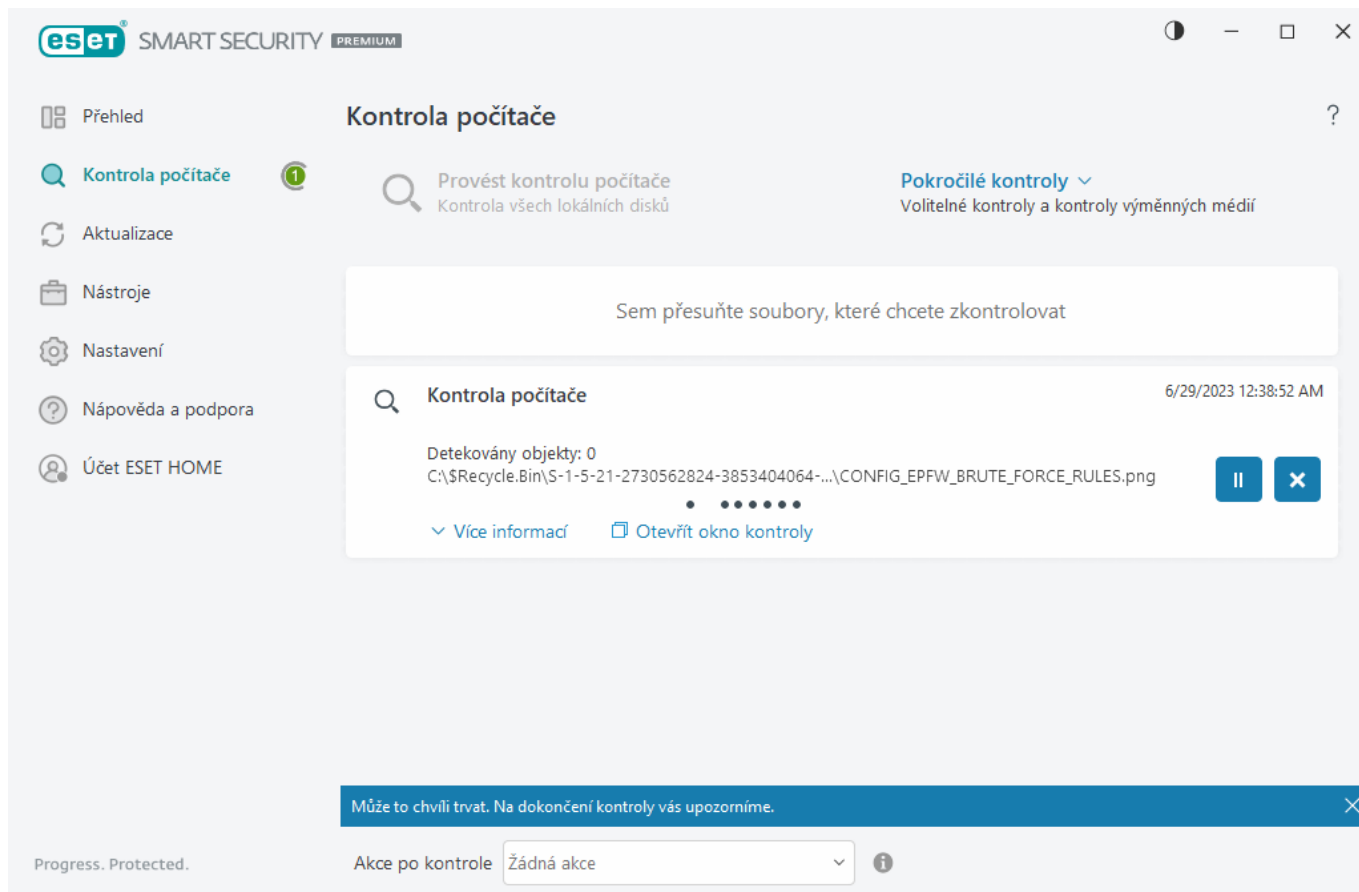
Ikona Stop – ukončí kontrolu.

Klepnutím na **Otevřít okno kontroly** otevřete [Protokol kontroly](#) s podrobnějšími informacemi o kontrole.

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



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



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

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



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

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

Protokol kontroly počítače

Podrobné informace týkající se určité kontroly můžete zobrazit v [Protokolech](#). Protokol kontroly obsahuje následující informace:

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



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

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

Kontrola počítače



Protokol kontroly

Verze detekčního jádra: 27487P (20230629)

Datum: 6/29/2023 Čas: 12:38:52 AM

Kontrolované disky, složky a soubory: Operační paměť;C:\Boot sektory/UEFI;C:\

User: DESKTOP-ILTJID9\User

Kontrola přerušena uživatelem.

Počet kontrolovaných objektů: 6901

Počet detekcí: 0

Čas ukončení: 12:39:04 AM Celkový čas kontroly: 12 sek (00:00:12)

☐ Filtrování

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

Kliknutím na přepínač ☐ **Filtrování** si zobrazíte dialogové okno, ve kterém můžete definovat kritéria [Filtrování protokolu](#) a vyhledávat v něm konkrétní záznamy. V kontextovém menu jednotlivých záznamů protokolu naleznete následující možnosti:

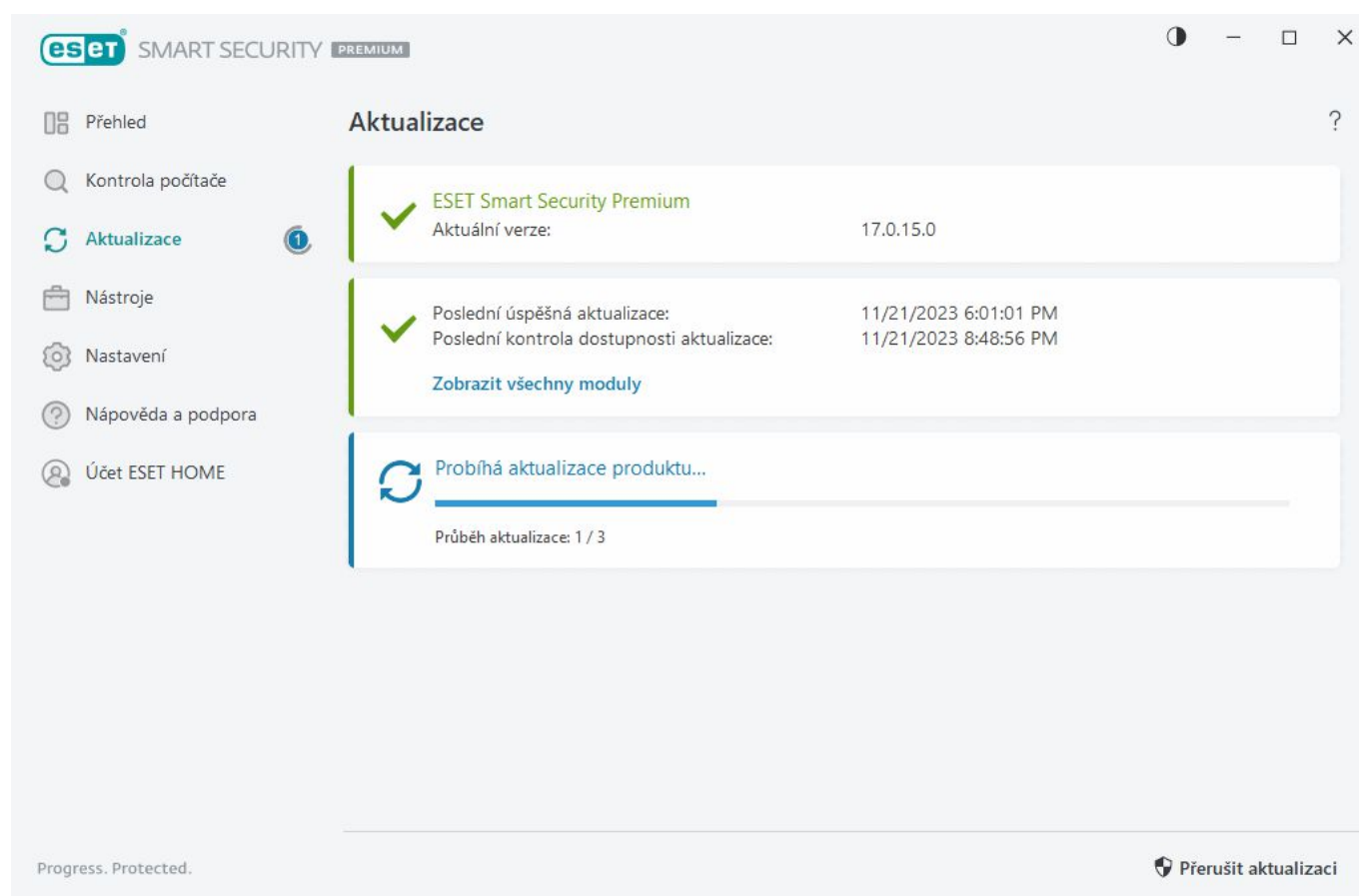
Akce	Použití
Filtrovat stejné záznamy	Aktivuje filtrování protokolu. V protokolu se následně zobrazí pouze záznamy stejného typu, odpovídající aktuálně vybranému záznamu.
Filtr	Tato možnost otevře okno Filtrování protokolu a umožňuje definovat kritéria pro konkrétní položky protokolu. Klávesová zkratka: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

Aktualizace

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

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

Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na tlačítko **Zkontrolovat aktualizace**. Pravidelná aktualizace modulů a komponent je důležitým aspektem pro zachování plné ochrany před škodlivým kódem. Věnujte prosím pozornost konfiguraci a práci modulů. Chcete-li dostávat aktualizace, je třeba produkt aktivovat pomocí aktivačního klíče. Pokud jste tak neučinili během instalace, je nutné [aktivovat ESET Smart Security Premium](#), abyste získali přístup k aktualizacím serverům společnosti ESET. Aktivační klíč vám byl zaslán e-mailem od společnosti ESET po zakoupení ESET Smart Security Premium.



Aktuální verze – zobrazuje číslo verze ESET programu, který máte nainstalován.

Poslední úspěšná aktualizace – zobrazuje datum, kdy se program naposledy aktualizoval. Pokud nevidíte dnešní datum, moduly produktu nemusí být aktuální.

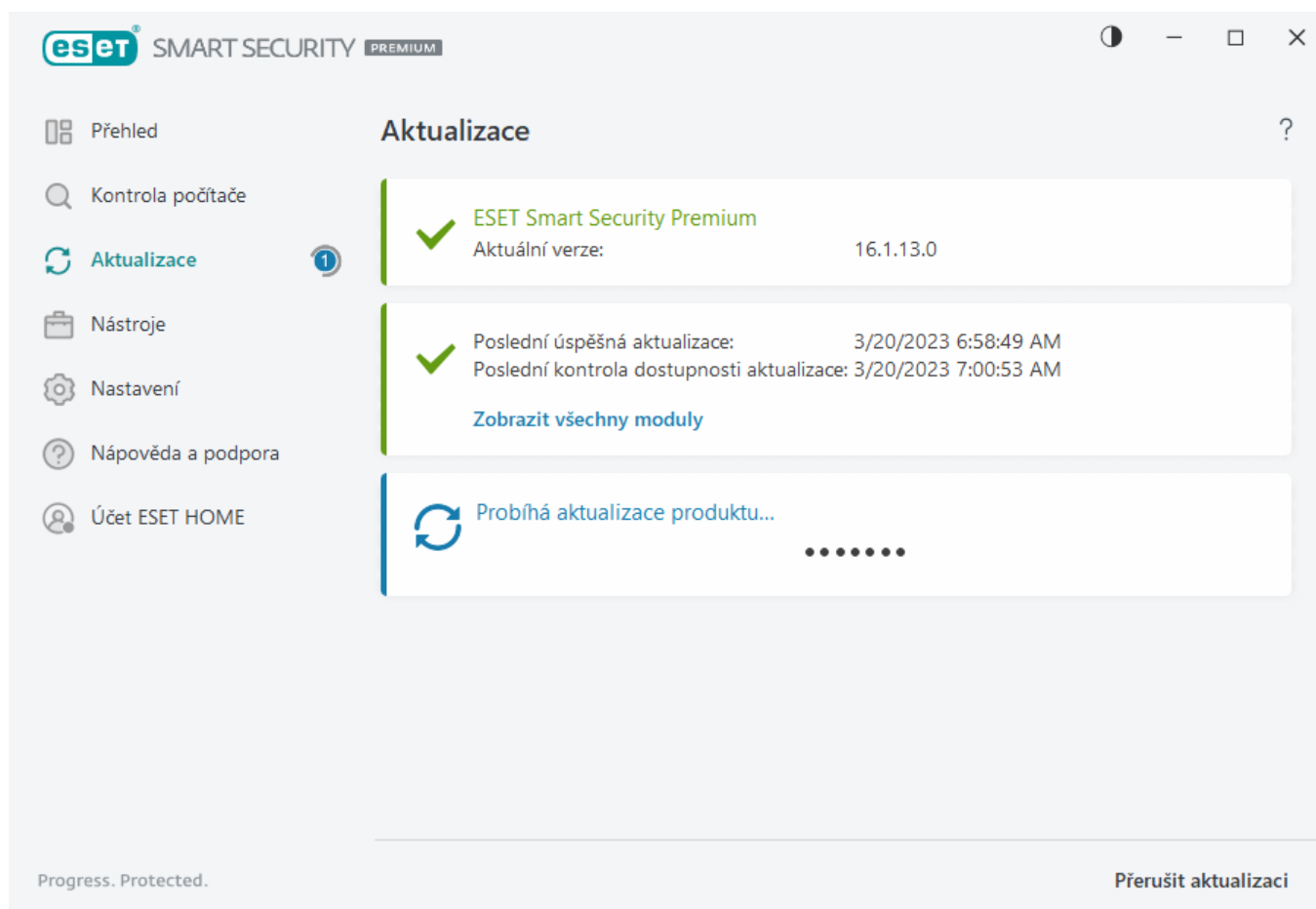
Poslední kontrola dostupnosti aktualizace – zobrazuje datum, kdy se program naposledy připojil k aktualizacím serverům a ověřil, zda není dostupná nová verze modulů.

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

Kliknutím na **Zkontrolovat aktualizace** zkontrolujte, zda máte nejnovější verzi ESET Smart Security Premium.

Průběh stahování

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



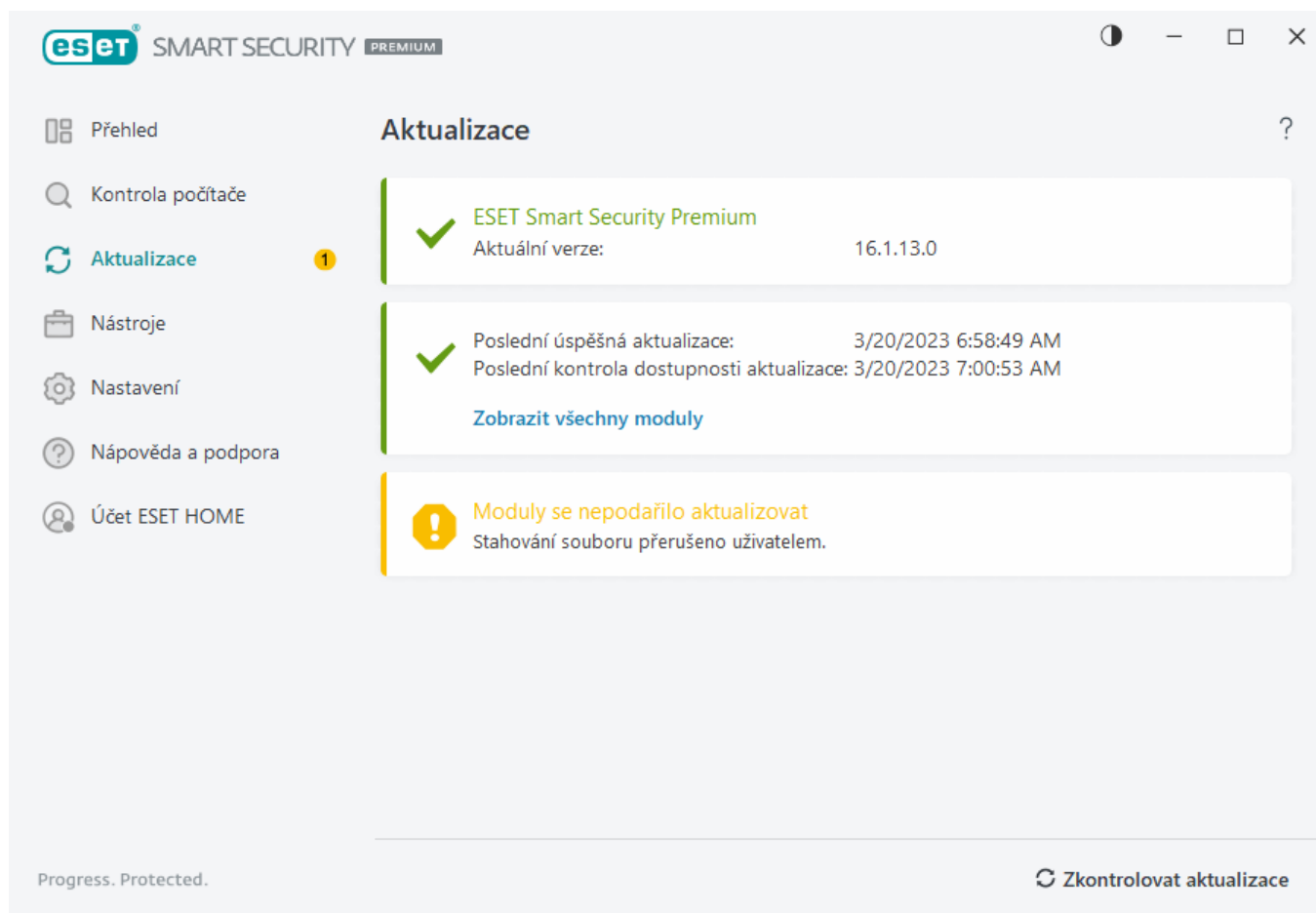
Za normálních okolností, při pravidelné a úspěšné stahování aktualizací, se v okně **Aktualizace** zobrazuje zelená fajfka. Pokud tomu tak není, program nepoužívá aktuální detekční moduly, čímž se zvyšuje riziko infiltrace. V takovém případě doporučujeme co nejdříve moduly aktualizovat.


Poslední úspěšná aktualizace

Pokud obdržíte informaci, že aktualizace modulů se nezdařila, může to být z následujících důvodů:

1. **Neplatné předplatné** – předplatné použité pro aktivaci je neplatné nebo vypršelo. V [hlavním okně programu](#) klikněte na **Nápověda a podpora > Změnit předplatné** a aktivujte produkt.
2. **Při pokusu o stažení souboru aktualizace došlo k chybě** – to může být způsobeno nesprávným [nastavením připojení](#). Doporučujeme, abyste vyzkoušeli připojení k internetu (otevřením jakékoli webové stránky ve webovém prohlížeči). Pokud se stránka nenačte, děje se tak v situaci, kdy počítač připojen k internetu není

nebo má problémy s připojením. Rovněž doporučujeme zkontrolovat, zda je počítač připojen k internetu, a ověřit, zda poskytovatel internetu nemá výpadek připojení.



 Po úspěšné aktualizaci ESET Smart Security Premium musíte restartovat vaše zařízení, aby se programové moduly aktualizovaly správně. Toto není vyložene nutné po aktualizaci programových modulů.

 Pro více informací přejděte do [ESET Databáze znalostí](#).

Dialogové okno – Vyžadován restart

Po aktualizaci ESET Smart Security Premium na novou verzi je vyžadován restart počítače. Nové verze ESET Smart Security Premium opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů.

Novou verzi ESET Smart Security Premium lze získat v [závislosti na nastavení aktualizace](#) automaticky nebo ručně [stažením a nainstalováním nejnovější verze](#) přes stávající.

Pro restartování počítače klikněte na **Restartovat nyní**. Pokud plánujete restartovat počítač později, klikněte na **Připomenout později**. Restart zařízení můžete provést ručně v [hlavním okně programu](#) na záložce **Přehled**.

Jak vytvořit aktualizací úlohu?

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

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

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

Každou z uvedených aktualizací úloh můžete upravit podle svých představ. Kromě standardních aktualizací úloh můžete vytvořit nové aktualizací úlohy s vlastním nastavením. Podrobněji se vytváření a nastavení aktualizací úloh zabýváme v kapitole [Plánovač](#).

Nástroje

Nabídka **Nástroje** obsahuje funkce, které nabízejí dodatečná zabezpečení a pomáhají zjednodušit správu ESET Smart Security Premium. K dispozici jsou následující nástroje:



[Protokoly](#)



[Spuštěné procesy](#) (pokud je ESET LiveGrid® v ESET Smart Security Premium zapnut)



[Bezpečnostní přehled](#)



[Síťová spojení](#) (pokud je na ESET Smart Security Premium zapnutý [Firewall](#))



[ESET SysInspector](#)



[Plánovač](#)



[Kontrola systému](#)



[Strážce sítě](#)



[Odeslat vzorek k analýze](#) (tato funkce nemusí být k dispozici, závisí na konfiguraci [ESET LiveGrid®](#)).

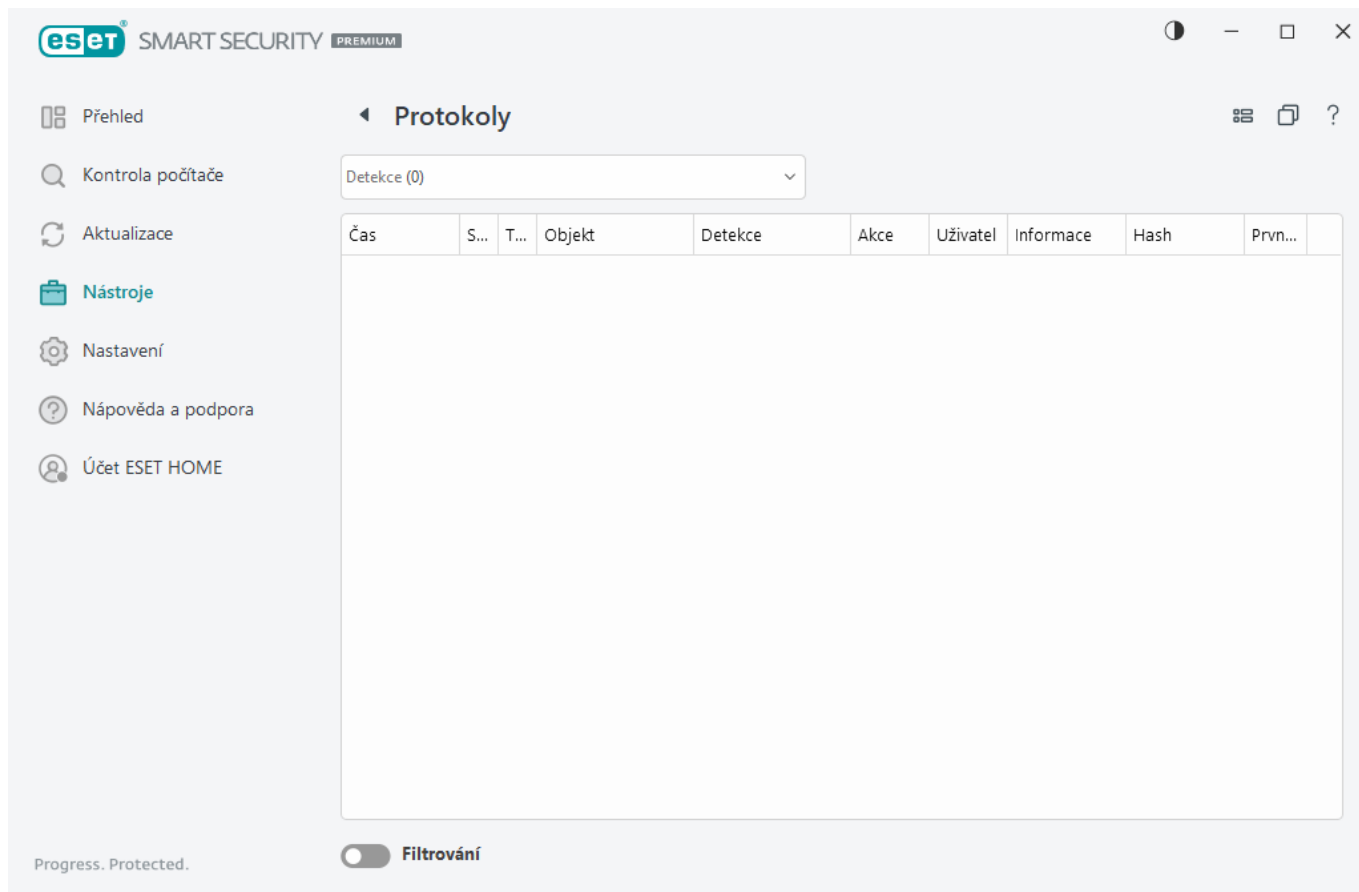


[Karanténa](#)



Protokoly

Do protokolů se zaznamenávají všechny důležité události programu, stejně tak v nich naleznete informace o detekovaných hrozbách. Záznamy v protokolech jsou důležitým zdrojem pro systémové analýzy, detekci hrozeb a řešení problémů. 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 i archivovat přímo v prostředí ESET Smart Security Premium.




Protokoly naleznete v [hlavním okně programu](#) > **Nástroje** > **Protokoly**. Následně z rozbalovacího menu Protokoly vyberte požadovaný typ protokolu:

- **Detekce** – protokol zachycených detekcí a infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly programu ESET Smart Security Premium. Informace v protokolu zahrnují čas detekce, skener, typ objektu, objekt, název detekce, uživatele přihlášeného v době detekce, informace o události, hash a první výskyt. Nevyléčené infiltrace jsou vždy označeny červeně na světle červeném pozadí. Vyléčené infiltrace jsou vždy označeny 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 Smart Security Premium a chybách, které se vyskytly. Protokol událostí obsahuje informace o událostech a chybách, ke kterým v programu došlo. Informace jsou určené systémovým administrátorům a uživatelům pro vyřešení problémů. Právě zde nejčastěji naleznete informace, které vám pomohou vyřešit problém vyskytující se v programu.
- **Kontrola počítače** – výsledky každé kontroly počítače se zobrazují v tomto okně. Každý řádek náleží samostatné kontrole. Dvojklikem na záznam se zobrazí [detaily vybrané kontroly](#).
- **Odeslané soubory** – seznam souborů odeslaných k analýze do ESET LiveGuard.
- **HIPS** – protokoly obsahují záznamy konkrétních [HIPS](#) pravidel, která se mají zaznamenávat. V protokolu je zobrazena aplikace, která danou operaci spustila, výsledek (tzn. zda bylo pravidlo povoleno, nebo zakázáno) a název pravidla.
- **Ochrana prohlížeče** – obsahuje záznamy o nepotvrzených nebo nedůvěryhodných souborech načtených ve webovém prohlížeči.
- **Síťová ochrana** – [protokol](#) obsahuje všechny vzdálené útoky zachycené Firewalllem, Ochranou proti

síťových útoků (IDS) a Ochranou proti zapojení do botnetu. 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. Analýza tohoto protokolu pomůže včas odhalit pokusy o nepovolený průnik do vašeho systému. Pro více informací o síťových útocích přejděte do kapitoly [IDS a pokročilé možnosti](#).

- **Filtrované webové stránky** – Tento seznam je užitečný, pokud chcete zobrazit seznam webových stránek, které byly zablokovány [Ochranou přístupu na web](#) nebo [Rodičovskou kontrolou](#). Protokol obsahuje informace o čase, URL adrese, uživateli a aplikaci, která se chtěla na konkrétní stránky připojit.
- **Antispamová ochrana poštovních klientů** – obsahuje záznamy související s e-mailovými zprávami, které byly označeny jako spam.
- **Rodičovská kontrola** – protokol zobrazuje webové stránky, které byly zablokovány nebo povoleny. Sloupce Typ vyhodnocení a Hodnota vyhodnocení informují o tom, jakým způsobem byla pravidla filtrování aplikována.
- **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. Můžete si také zobrazit podrobnosti, jako je typ zařízení, sériové číslo, název dodavatele a velikost média (je-li k dispozici).
- **Ochrana webkamery** – obsahuje záznamy o aplikacích, kterým byl zablokován přístup k webkameře.

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 klávesu **CTRL** nebo **SHIFT** a proveďte výběr zájmových položek.


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 aktivování 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** – zkopíruje vybrané/všechny záznamy z daného okna.
- **Kopírovat buňku** – zkopíruje obsah buňky, na kterou jste v tabulce protokolů klikli pravým tlačítkem myši.
- **Odstranit/Odstranit vše** – odstraní vybrané nebo všechny zobrazené záznamy. Tato akce vyžaduje administrátorská oprávnění.

- **Exportovat.../Exportovat vše** – po kliknutí uložíte vybrané záznamy do souboru v XML formátu.
- **Hledat.../Hledat další.../Hledat předchozí...** – po kliknutí můžete definovat kritéria pro konkrétní záznamy pomocí Filtrování protokolu.
- **Popis detekce** – po kliknutí budete přesměrováni do ESET Encyklopedie hrozeb, kde naleznete informace o jednotlivých hrozbách.
- **Vytvořit výjimku** – kliknutím spustíte [průvodce vytvořením detekční výjimky](#) (tato možnost není dostupná pro objekty detekované jako malware).
- **Přidat do seznamu povolených souborů v Ochráně prohlížeče** – otevře [Seznam povolených souborů v Ochráně prohlížeče](#) a přidá položku do seznamu.

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. Umožňuje zúžit záznamy protokolu, například pokud hledáte konkrétní typ události, stav nebo časové období. Záznamy protokolu lze filtrovat pomocí výběru určitých hodnot ve vyhledávání. Ve výsledcích se následně zobrazí hodnoty, které jsou pro nastavená kritéria relevantní.

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

Hledat text

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

Hledat ve sloupcích

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

Typy záznamů

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

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informační** – jedná se o informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíše 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.

Spuštěné procesy

Tento nástroj zobrazuje spuštěné programy a procesy a umožňuje společnosti ESET získávat informace o nových infiltracích. ESET Smart Security Premium poskytuje detailnější informace o spuštěných procesech díky technologii [ESET LiveGrid®](#) pro zajištění lepší ochrany uživatelů.

SMART SECURITY PREMIUM

Přehled

Kontrola počítače

Aktualizace

Nástroje

Nastavení

Nápověda a podpora

Účet ESET HOME

Spuštěné procesy

V tomto okně jsou zobrazeny vybrané soubory spolu s doplňkovými informacemi z ESET LiveGrid®. Seznam poskytuje informace o úrovni rizika daného souboru, počtu uživatelů a datu prvního výskytu.

Úroveň rizi...	Proces	PID	Počet uživatelů	První výskyt	Název aplikace
	smss.exe	364		před 2 lety	Microsoft® Windows® Op...
	csrss.exe	468		před 2 lety	Microsoft® Windows® Op...
	wininit.exe	548		před 6 měsíci	Microsoft® Windows® Op...
	winlogon.exe	620		před měsícem	Microsoft® Windows® Op...
	services.exe	692		před 3 měsíci	Microsoft® Windows® Op...
	lsass.exe	700		před 6 měsíci	Microsoft® Windows® Op...
	svchost.exe	820		před rokem	Microsoft® Windows® Op...
	fontdrvhost.exe	848		před 3 měsíci	Microsoft® Windows® Op...
	dwm.exe	420		před 2 lety	Microsoft® Windows® Op...
	wudfhost.exe	1488		před 6 měsíci	Microsoft® Windows® Op...
	vboxservice.exe	1580		před 2 lety	Oracle VM VirtualBox Guest...
	efwd.exe	1592		právě teď	ESET Security
	dlpsrv.exe	2296		před 6 měsíci	ESET Secure Data
	spoolsv.exe	2940		před 3 měsíci	Microsoft® Windows® Op...
	akvcamassistant.exe	3128		před 2 lety	AkVCamAssistant
	sihost.exe	4084		před 2 lety	Microsoft® Windows® Op...
	googleupdate.exe	2804		před 2 lety	Google Update
	taskhostw.exe	2708		před 6 měsíci	Microsoft® Windows® Op...
	ctfmon.exe	5260		před 2 lety	Microsoft® Windows® Op...
	explorer.exe	5492		před měsícem	Microsoft® Windows® Op...

Progress. Protected.

Úroveň rizika – ve většině případů přiřazuje ESET Smart Security Premium 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 1 – V pořádku (zelený) až po 9 – Nebezpečný (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**.

i Známé aplikace označené zeleně a jsou považovány za důvěryhodné. Proto pro zvýšení výkonu kontroly nebudou kontrolovány.

PID – ID běžícího procesu v operačním systému Windows. Slouží jako parametr při volání různých funkcí, jako je nastavení priority procesů (pro zkušené uživatele).

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®.

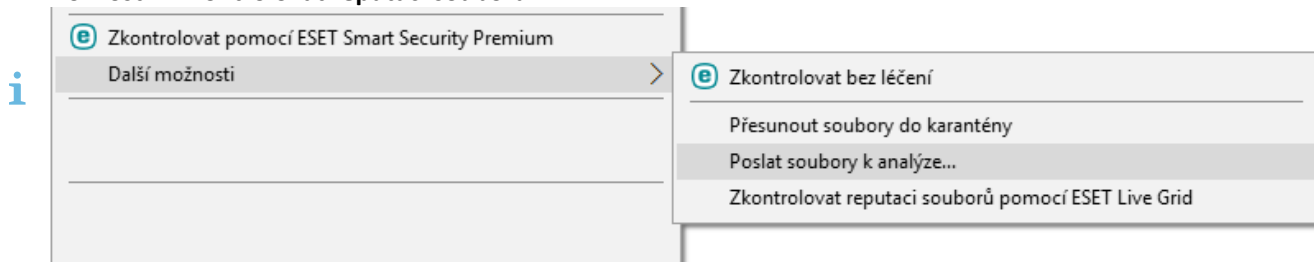
i V případě, že je aplikace označena jako Neznámá (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete [soubor odeslat k analýze](#) do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde o aplikaci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

Název aplikace – název aplikace nebo procesu.

Po kliknutí na konkrétní aplikaci si zobrazíte 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/Upraveno** – datum a čas, kdy byla aplikace vytvořena.

Úroveň rizika 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 souboru**.



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 zjištěných infikovaných e-mailových [objektů](#).
- **Webové stránky zablokované Rodičovskou kontrolou** – zobrazuje počet stránek zablokovaných [rodičovskou kontrolou](#).
- **Detekované PUA** – zobrazuje počet detekovaných [potenciálně nechtěných aplikací](#) (PUA).
- **Detekovaných nevyžádaných e-mailů** – zobrazuje počet detekovaných spamů.
- **Zablokované přístupy k webové kameře** – zobrazuje počet zablokovaných přístupů k webové kameře.
- **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 e-mailových objektů.


- **Soubory analyzované prostřednictvím ESET LiveGuard** – zobrazuje počet vzorků analyzovaných službou [ESET LiveGuard](#).

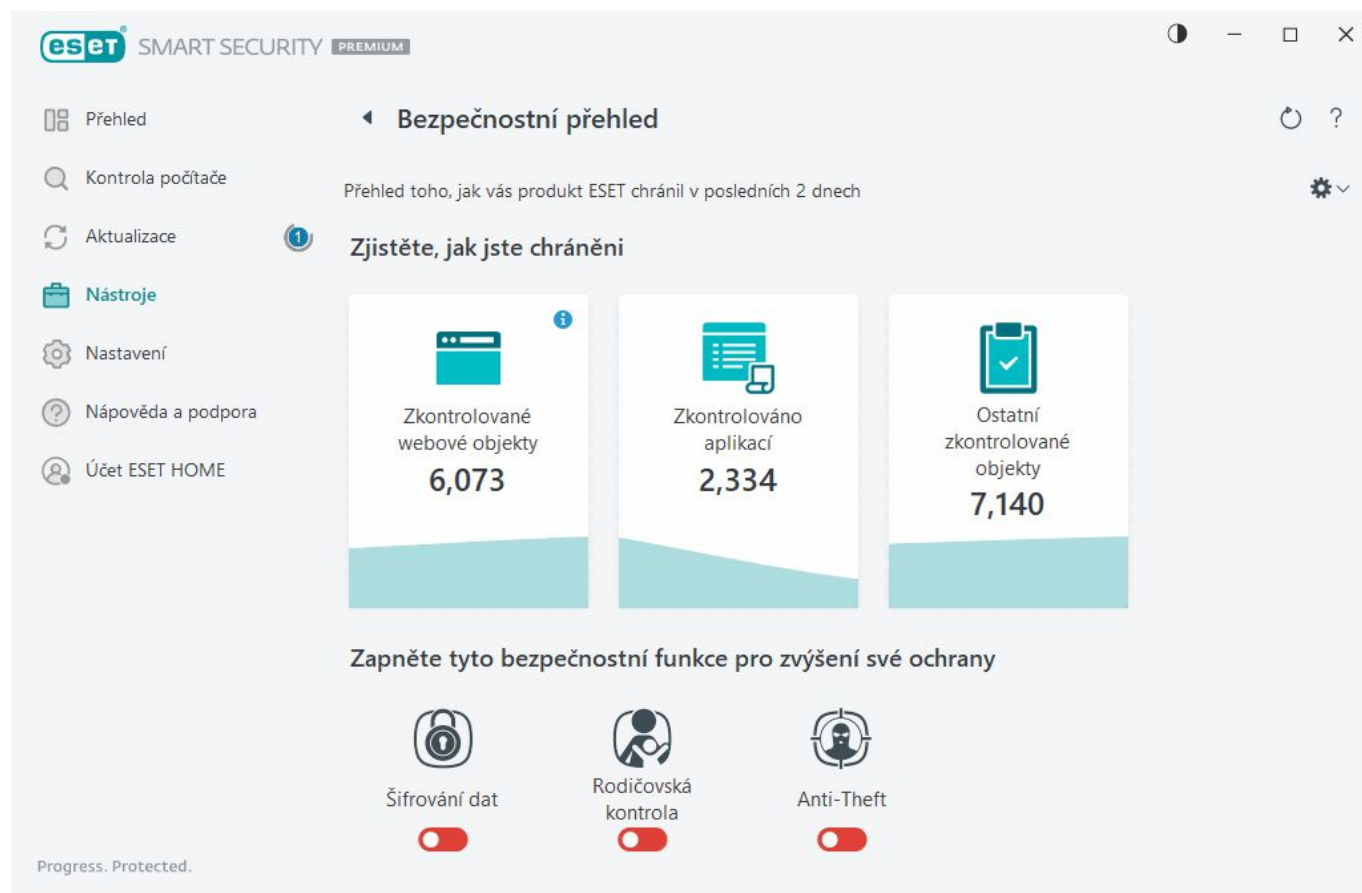
Pořadí výše uvedených kategorií se dynamicky mění. Na prvním místě jsou vždy zobrazeny kategorie s nejvyššími hodnotami. Kategorie obsahující nulové hodnoty se nezobrazují. Pro zobrazení dalších kategorií klikněte na **Zobrazit více**.

Poslední část Bezpečnostního přehledu umožňuje aktivovat následující funkce:

- [ESET LiveGuard](#)
- [Secure Data](#)
- [Rodičovská kontrola](#)
- [Anti-Theft](#)

Jakmile některou z výše uvedených funkcí zapnete, nebude se již zobrazovat v bezpečnostním přehledu jako nefunkční.

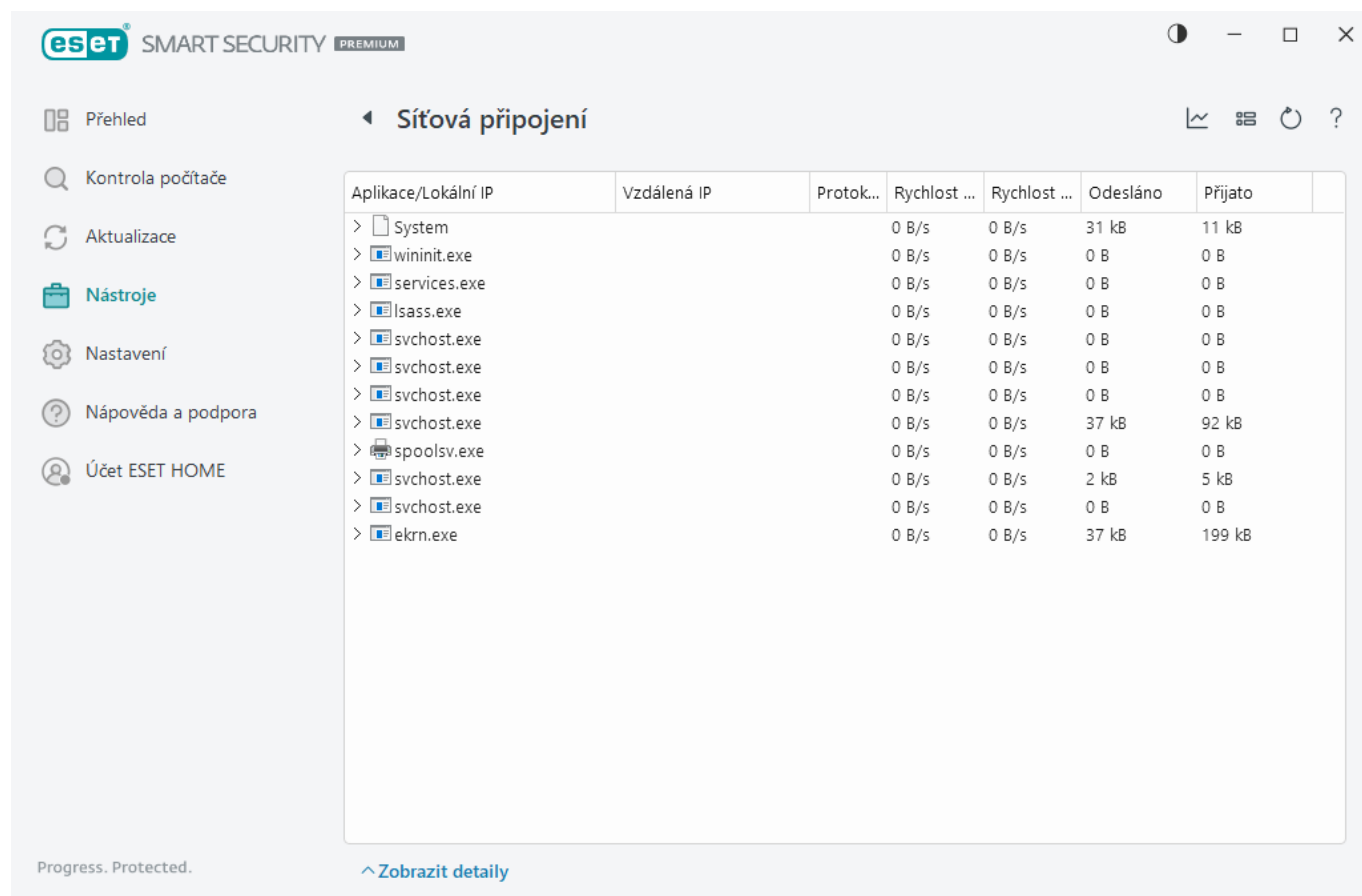
Kliknutím na ozubené kolečko  v pravém horním rohu můžete **zapnout/vypnout upozornění na bezpečnostní přehled**, případně si zobrazit data za posledních 30 dní, resp. od aktivace produktu. Pokud jste produkt ESET Smart Security Premium nainstalovali před méně než 30 dny, zobrazí se pouze data od instalace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

Síťová spojení

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



Aplikace/Lokální IP	Vzdálená IP	Protok...	Rychlost ...	Rychlost ...	Odesláno	Přijato
> System			0 B/s	0 B/s	31 kB	11 kB
> wininit.exe			0 B/s	0 B/s	0 B	0 B
> services.exe			0 B/s	0 B/s	0 B	0 B
> lsass.exe			0 B/s	0 B/s	0 B	0 B
> svchost.exe			0 B/s	0 B/s	0 B	0 B
> svchost.exe			0 B/s	0 B/s	0 B	0 B
> svchost.exe			0 B/s	0 B/s	0 B	0 B
> svchost.exe			0 B/s	0 B/s	37 kB	92 kB
> spoolsv.exe			0 B/s	0 B/s	0 B	0 B
> svchost.exe			0 B/s	0 B/s	2 kB	5 kB
> svchost.exe			0 B/s	0 B/s	0 B	0 B
> ekern.exe			0 B/s	0 B/s	37 kB	199 kB

Kliknutím na ikonu grafu  si zobrazíte přehled [síťové aktivity](#).

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

Sloupce

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

Vzdálená IP – IP adresa a port vzdáleného počítače.

Protokol – použitý transportní protokol.

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

Odesláno/Přijato – celkový objem přijatých a odeslaných dat.

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

Kliknutím pravým tlačítkem na spojení se zobrazí následující možnosti:

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

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

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

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

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


Aktualizovat nyní – kliknutím aktualizujete obsah okna **Síťová spojení**.

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

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

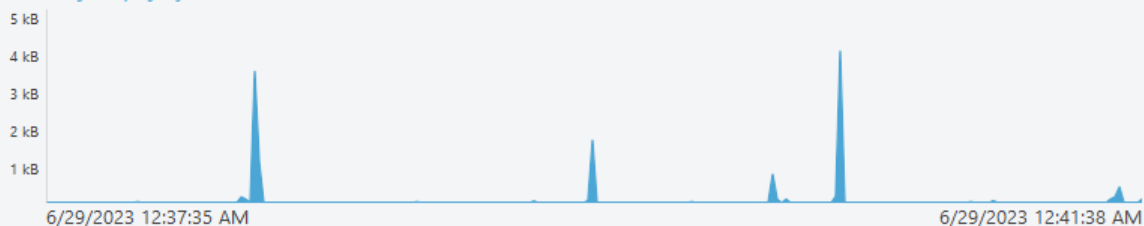
Dočasně povolit komunikaci pro daný proces – aktuální spojení aplikace bude povoleno. Při vytvoření nového spojení se aplikuje předdefinované pravidlo firewallu. Popis nastavení naleznete v kapitole [Pravidla firewallu](#).

Síťová aktivita

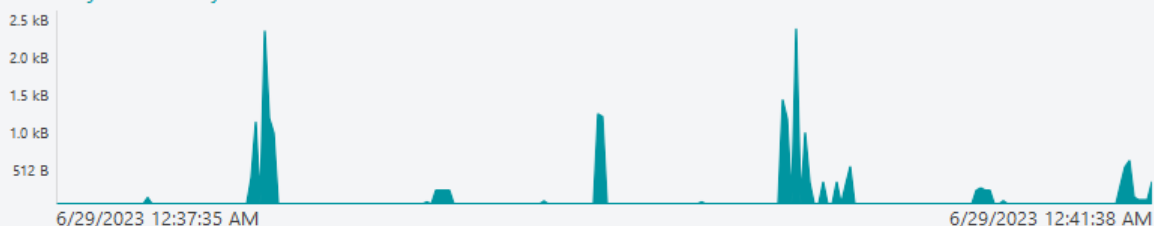
Pro zobrazení **Síťové aktivity** ve formě grafu klikněte na záložce **Nástroje > Síťová spojení** na ikonu grafu . Na základě vybrané rychlosti aktualizace se ve spodní části grafu zobrazuje časová osa, kde je zaznamenána síťová aktivita souborového systému v reálném čase. Ve spodní části se zobrazuje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

Síťová aktivita

Objem přijatých dat



Objem odeslaných dat



Rychlost aktualizace

1 sekunda

K dispozici jsou následující možnosti:

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

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

ESET SysInspector

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

V okně ESET SysInspector se nachází informace o vytvořených protokolech:

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

Dostupné jsou následující akce:

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

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

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

Plánovač

Plánovač spravuje a spouští naplánované úlohy s předem nakonfigurovaným nastavením.

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

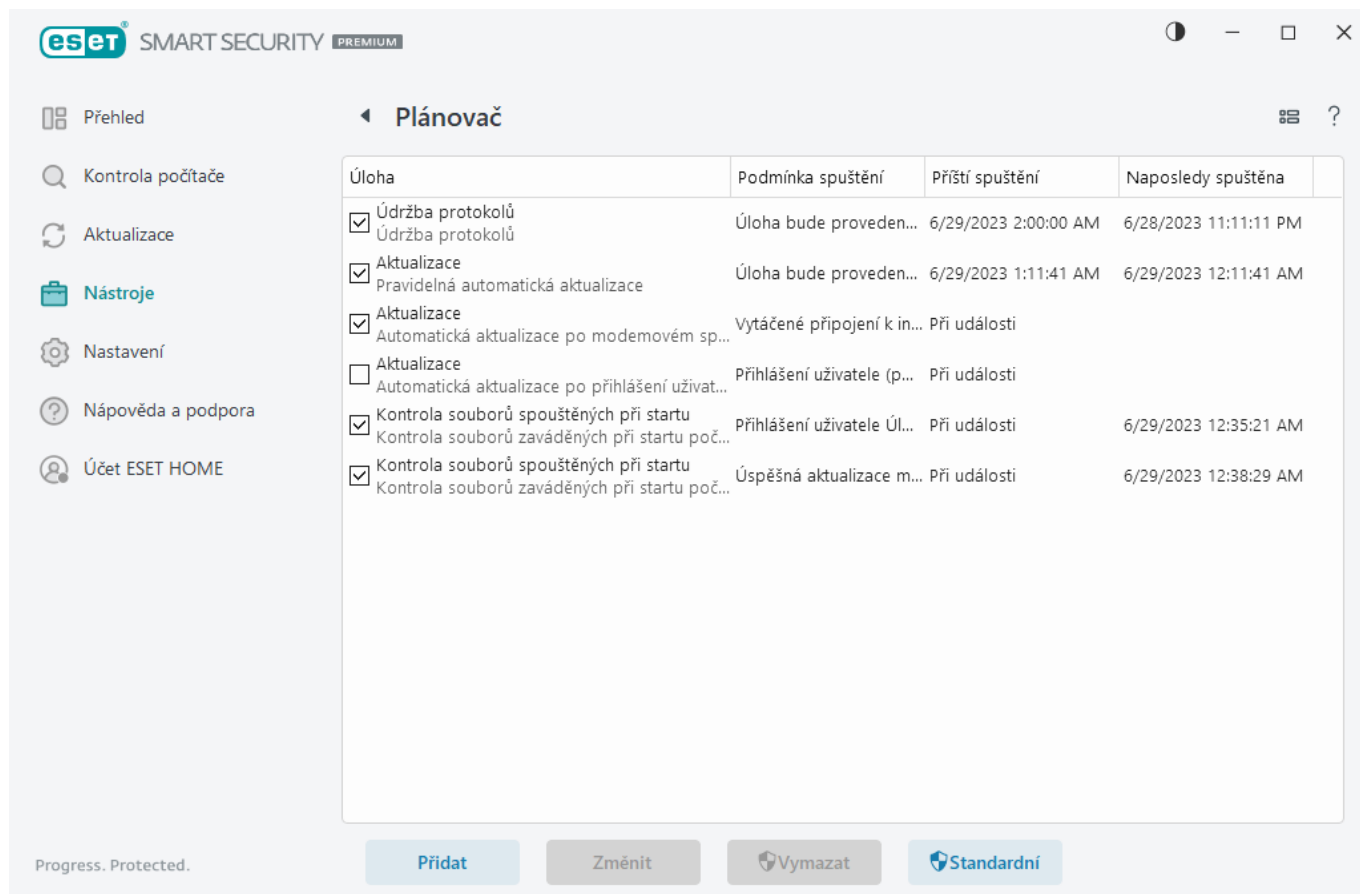
Plánovač slouží k plánování úloh jako je např. aktualizace programu, kontrola počítače, kontrola souborů spouštěných po startu nebo pravidelná údržba protokolů. Přímou v hlavním okně Plánovače můžete pomocí tlačítek **Přidat** a **Odstranit** úlohy vytvářet nebo mazat. Všechny vámi provedené změny zahodíte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

Standardně **Plánovač** zobrazuje následující naplánované úlohy:

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

- **Kontrola souborů spouštěných při startu** (při úspěšné aktualizaci detekčního jádra).

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**.



Úloha	Podmínka spuštění	Příští spuštění	Naposledy spuštěna
<input checked="" type="checkbox"/> Údržba protokolů Údržba protokolů	Úloha bude proveden...	6/29/2023 2:00:00 AM	6/28/2023 11:11:11 PM
<input checked="" type="checkbox"/> Aktualizace Pravidelná automatická aktualizace	Úloha bude proveden...	6/29/2023 1:11:41 AM	6/29/2023 12:11:41 AM
<input checked="" type="checkbox"/> Aktualizace Automatická aktualizace po modemu sp...	Vytáčené připojení k in...	Při události	
<input type="checkbox"/> Aktualizace Automatická aktualizace po přihlášení uživat...	Přihlášení uživatele (p...	Při události	
<input checked="" type="checkbox"/> Kontrola souborů spouštěných při startu Kontrola souborů zaváděných při startu poč...	Přihlášení uživatele Úl...	Při události	6/29/2023 12:35:21 AM
<input checked="" type="checkbox"/> Kontrola souborů spouštěných při startu Kontrola souborů zaváděných při startu poč...	Úspěšná aktualizace m...	Při události	6/29/2023 12:38:29 AM

Přidání nové úlohy

1. Klikněte na tlačítko **Přidat** ve spodní části okna.
2. Zadejte název úlohy.
3. 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 detekčních a programových modulů.

4. Pro aktivování úlohy přepněte přepínač do polohy **Zapnuto** (to můžete udělat kdykoli později přímo v seznamu naplánovaných úloh) 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 doba od posledního spuštění překročí (v hodinách)** – jedná se o časové období, které uplyne od doby, kdy měla být úloha spuštěna poprvé. Pokud dojde k překročení této doby, úloha se okamžitě spustí. Čas definujte pomocí zobrazeného číselníku.

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

Možnosti naplánované kontroly

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

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

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

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

- **Žádná akce** – po dokončení kontroly se neprovede žádná akce.
- **Vypnout** – počítač se po dokončení kontroly vypne,
- **Restartovat v případě potřeby** – počítač se po dokončení kontroly restartuje, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.
- **Restartovat** – počítač se po dokončení kontroly restartuje.
- **V případě potřeby vynutit restart** – po dokončení kontroly se vynutí restartování počítače, pokud je to potřeba pro dokončení léčení detekovaných hrozeb.

- **Vynutit restart** – po dokončení kontroly dojde k automatickému zavření všech otevřených aplikací a počítač se restartuje.
- **Režim spánku** – aktuální relace se uloží do operační paměti a počítač přejde do úsporného stavu. Následné probuzení počítače je rychlé a můžete ihned pokračovat v rozdělené činnosti.
- **Hibernovat** – uloží aktuální relaci na pevný disk a počítač se kompletně vypne. Při další spuštění počítače se obnoví poslední stav.

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

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

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

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

Další informace naleznete v kapitole [Průběh kontroly](#).

Informace o naplánované úloze

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

Detaily úlohy

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

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

Provedení úlohy

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

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

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

Provedení úlohy – Jednou

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

Provedení úlohy – Denně

Úloha bude provedena každý den ve stanovený čas.

Provedení úlohy – Týdně

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

Provedení úlohy – Při události

Úloha bude provedena při jedné z následujících událostí:

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

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

Neprovedení úlohy

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

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

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

✓ V příkladu je úloha nastavena tak, aby se spouštěla opakovaně každou hodinu. V poli **Okamžitě, pokud od posledního provedení uplynul stanovený interval (v hodinách)** je nastavena hodnota 2 hodiny. Úloha se spustí ve 13:00 a po dokončení počítač přejde do režimu spánku:

- Počítač se probudí v 15:30. K prvnímu vynechanému spuštění úlohy došlo ve 14:00. Od 14:00 uplynulo pouze 1,5 hodiny, takže úloha bude spuštěna v 16:00.
- Počítač se probudí v 16:30. K prvnímu vynechanému spuštění úlohy došlo ve 14:00. Od 14:00 uplynuly 2,5 hodiny, takže se úloha spustí okamžitě.

Detaily úlohy – Aktualizace

Chcete-li program aktualizovat ze dvou aktualizčních serverů, je nutné vytvořit dva různé profily aktualizace. Pokud se vám nepodaří stáhnout aktualizční soubory, program se automaticky přepne na alternativní. Tuto možnost můžete použít například pro notebooky, které jsou aktualizovány z lokálních LAN aktualizčních serverů a zároveň jsou uživatelé často přistupují k internetu. V případě neúspěšné aktualizace z hlavního profilu s nastavením pro lokální LAN, se aktualizace provede pomocí alternativního profilu nastaveného pro aktualizaci přímo ze serverů společnosti ESET.

Detaily úlohy – Spuštění aplikace

Pomocí tohoto typu úlohy si můžete naplánovat spuštění externí aplikace.

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

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

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

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

Kontrola systému

Kontrola systému je nástroj pomáhající obnovit správný chod počítače po odstranění hrozby. Škodlivý kód může v některých případech zakázat přístup k systémovým součástem jako je například Editor registru, Správce úloh nebo Windows Update. Kontrola systému obnoví přednastavené hodnoty v jednom kliku.

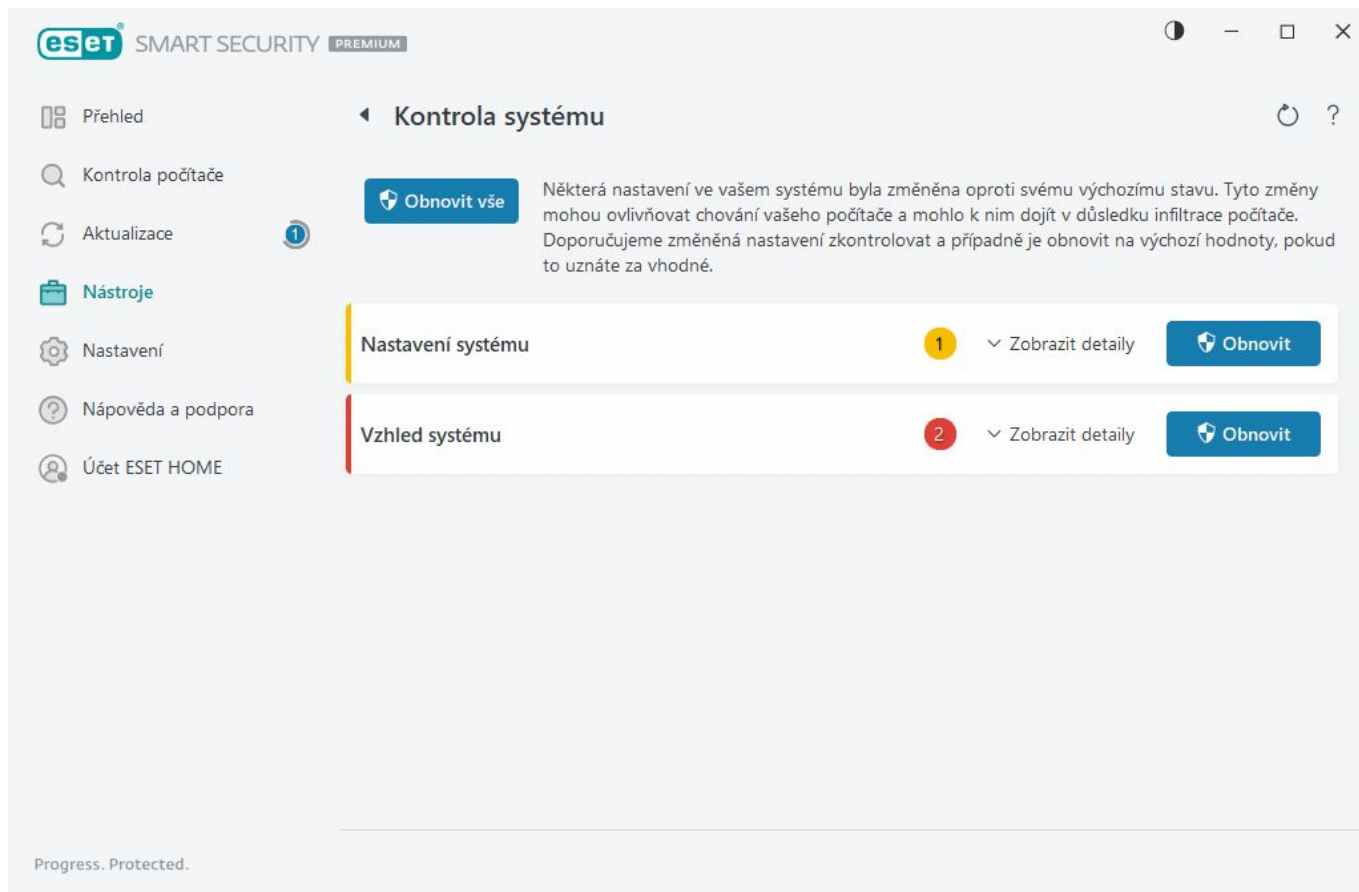
Použitím tohoto nástroje obnovíte klíčová nastavení systému na výchozí hodnoty:

- **Nastavení zabezpečení:** upozorníme vás na změny, které mohou způsobit vyšší zranitelnost vašeho počítače (například nevhodná konfigurace Windows Update),
- **Nastavení systému:** upozorníme vás na změny, které mají dopad na chování operačního systému (například asociace souborů),
- **Vzhled systému:** upozorníme vás na změny v nastavení, které ovlivňují vzhled systému (například možnosti pro konfiguraci pozadí plochy),
- **Vypnuté funkce:** upozorníme vás na funkce a aplikace, které jsou vypnuté,
- **Obnovení systému Windows:** nastavení funkce, které umožňuje obnovit operační systém Windows do předchozího stavu.

Kontrola systému se může spustit:

- po detekci hrozby
- pokud uživatel klikne na **Obnovit**

Zkontrolujte změny a případně obnovte nastavení.



i Tento nástroj může použít pouze uživatel s administrátorským oprávněním.

Strážce sítě

Strážce sítě vám pomůže najít ve vámi označené síti jako důvěryhodné (například domácí nebo firemní síti) zranitelnosti, jako jsou otevřené porty nebo slabé heslo k routeru. Dokáže zobrazit všechna zařízení připojená do vaší domácí sítě a roztřídit je dle typů (např. tiskárny, telefony, herní konzole a další chytrá zařízení aj.).

Tento modul vám pomůže identifikovat zranitelnosti ve vašem domácím routeru a zvýší úroveň zabezpečení při připojení do sítě.

Strážce sítě nemůže v žádném případě ovlivnit konfiguraci vašeho routeru. Veškeré změny v konfiguraci musíte provést osobně prostřednictvím nástrojů dodávaných výrobcem síťového zařízení. Domácí routery se dostávají do hledáčku autorů škodlivých kódů, protože kvůli bezpečnostním zranitelnostem je snadné je ovládnout, a následně mohou být zneužitelné pro DDoS útoky, případně vás směřovat na podvodné stránky. Pokud jako uživatel nezměníte přednastavené heslo routeru, stává se snadným terčem pro útok hackerů. Pro hackery je snadné takové heslo uhodnout, následně se přihlásit k vašemu routeru a překonfigurovat nebo kompromitovat vaši síť.



Pro přístup do administrace routeru byste měli používat silná a dostatečně dlouhá hesla, která by se měla skládat ze znaků, čísel a speciálních symbolů, a ideálně kombinovat malá a velká písmena. Jedině tak budete mít jistotu, že heslo bude velmi těžké uhodnout a prolomit.


Pokud je síť, ke které jste připojeni, [nakonfigurována jako důvěryhodná](#), můžete si ji označit štítkem "Moje síť". Štítek k síti přidáte kliknutím na možnost **Označit jako "Moje síť"**. Tento štítek se zobrazí vedle názvu sítě napříč produktem ESET Smart Security Premium, abyste měli lepší přehled o zabezpečení. Pro odebrání štítku klikněte na **Zrušit označení "Moje síť"**.

Zařízení připojená do sítě se standardně zobrazují v seznamu se základními informacemi o nich. Kliknutím na řádek tabulky si zobrazíte [detailní informace o zařízení](#).

V režimu seznamu můžete pomocí rozbalovacího menu **Sítě** filtrovat zařízení dle následujících kritérií:

- Zařízení připojená do **konkrétní sítě**
- Zařízení připojená do **Všech sítí**
- Nerozpoznaná zařízení

Kliknutím na ikonu zařízení si zobrazíte [detailní informace o zařízení](#). Pro snadnější identifikaci jsou nedávno připojená zařízení zobrazena blíže středu.

Kliknutím na ozubené kolečko  v pravém horním rohu vyberte, zda chcete dostávat oznámení, když v síti objeví nové zařízení.

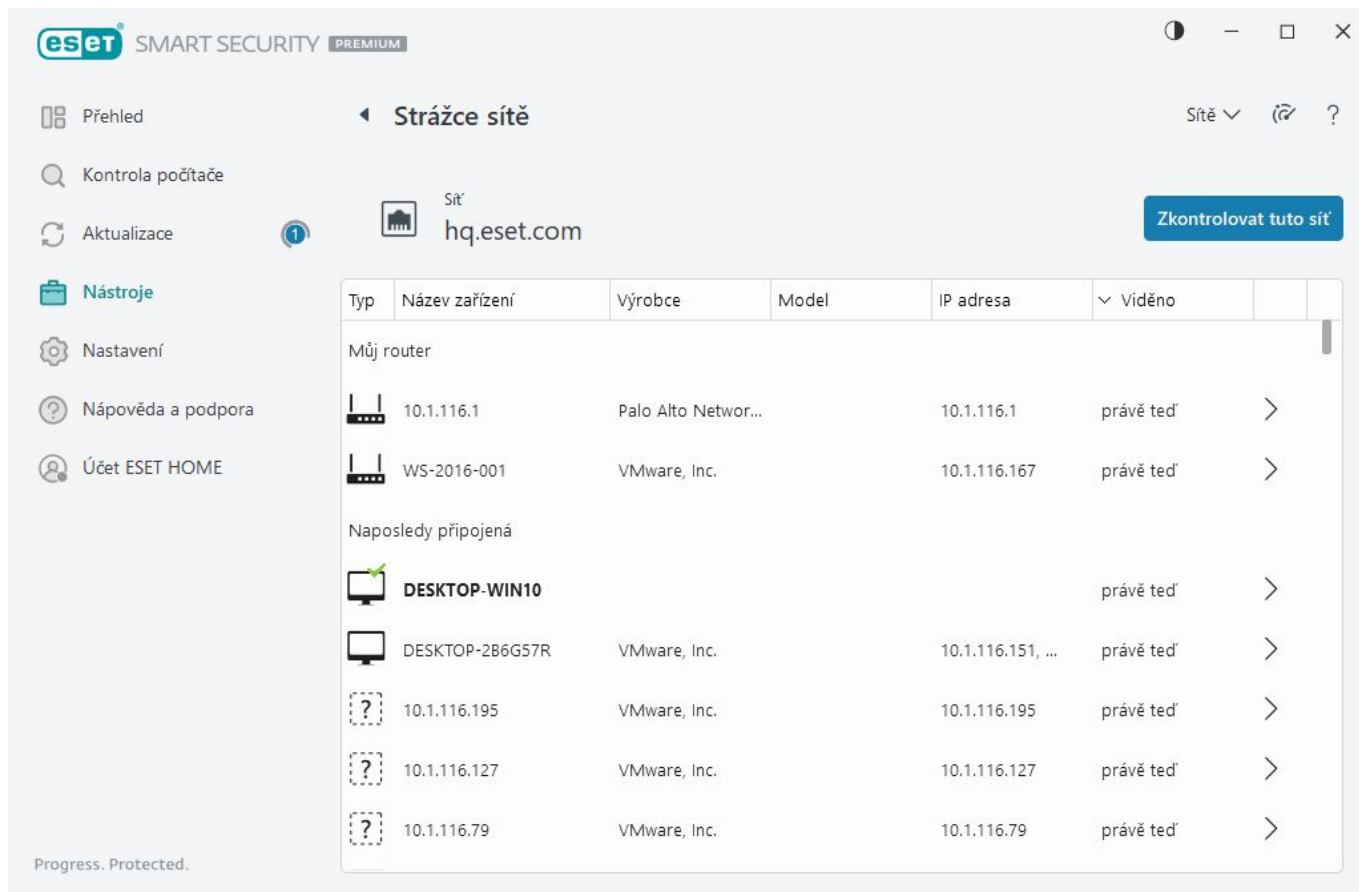
Kontrolu zabezpečení routeru spustíte kliknutím na tlačítko **Zkontrolovat tuto síť**. Následně se rozhodněte, co chcete zkontrolovat. Tlačítko **Zkontrolovat tuto síť** je dostupné pouze pro síť označené jako důvěryhodné. Chcete-li zkontrolovat nebo upravit nastavení sítě, podívejte se do kapitoly [Profily síťového připojení](#).

K dispozici jsou následující možnosti:

- Zkontrolovat všechna zařízení
- Zkontrolovat pouze router
- Zkontrolovat pouze zařízení



Tento typ kontroly spouštějte výhradně v sítích, které znáte. Pokud spustíte kontrolu v jiných nedůvěryhodných sítích, může takový test nést rizika.



Po dokončení kontroly routeru se zobrazí v bublina, ve které je uveden odkaz na zobrazení výsledku kontroly. Pro zobrazení naposledy blokové komunikace klikněte na **Řešení problémů**. Pro více informací přejděte do kapitoly [Řešení problémů s firewallem](#).

Modul Strážce sítě zobrazuje dva typy oznámení:

- **Nové zařízení ve vaší síti** – upozornění se zobrazí v případě, kdy jste připojeni do sítě, a připojí se do ní nové zařízení.
- **Nalezeno nové zařízení v síti** – upozornění se zobrazí v případě, když se připojíte do důvěryhodné sítě a od vašeho posledního připojení se v síti objevilo nové zařízení.

i V obou případech budete upozorněni, pokud se neautorizované zařízení připojí do vaší sítě. Pro zobrazení detailnější informací klikněte v zobrazením oznámení na možnost **Zobrazit informace o zařízení**.

Co znamenají ikony zařízení ve funkci Strážce sítě?

	– Ikona žluté hvězdy indikuje zařízení, která jsou v síti nová nebo která byla programem ESET nalezená poprvé.
	– Žlutá upozorňující ikona indikuje, že router může obsahovat zranitelnosti. Klikněte na ikonku pro zobrazení detailnějších informací o problému.
	– Červená varující ikona indikuje, že router může obsahovat zranitelnosti a může být infikovaný. Klikněte na ikonku pro zobrazení detailnějších informací o problému.
	– Modrá ikonka se může zobrazit v případě, kdy má pro vás produkt ESET doplňující informace o vašem routeru, ale nevyžaduje okamžitou pozornost, protože se nejedná o bezpečnostní problém. Klikněte na ikonku pro zobrazení detailnějších informací.

Síťové zařízení ve Strážci sítě

Zde naleznete detailní informace o konkrétním síťovém zařízení, jako:

- Název zařízení
- Typ zařízení
- Naposledy viděno
- Název sítě
- IP adresa
- MAC adresa
- Operační systém

Kliknutím na ikonu tužky můžete zařízení přejmenovat, případně změnit jeho typ.

Odstranit z historie – kliknutím odstraníte zařízení ze seznamu zařízení. Tato možnost je k dispozici pouze pro zařízení, která nejsou právě připojena k síti.

Pro každý typ zařízení jsou dostupné následující akce:

✓ [Router](#)

Nastavení routeru – Otevřete nastavení routeru z webového rozhraní, mobilní aplikace nebo klikněte na **Otevřít rozhraní routeru**. Pokud používáte router, který vám byl zapůjčen poskytovatelem internetu, pro opravu detekovaných bezpečnostních problémů bude zřejmě nutné kontaktovat technickou podporu poskytovatele služby nebo výrobce routeru. Vždy proveďte bezpečnostní opatření, jak je popsáno ve vaší uživatelské příručce.

Ochrana – K ochraně vašeho routeru a sítě před kybernetickými útoky postupujte dle základních uvedených doporučení.

✓ [Síťové zařízení](#)

Identifikace zařízení – Pokud si nejste jisti zařízením připojeným do vaší sítě, zkontrolujte jméno výrobce v názvu zařízení. Může vám to pomoci určit, o jaký druh zařízení se jedná. Pro pozdější identifikaci můžete změnit jméno zařízení.

Odpojení zařízení – Pokud si nejste jisti, zda je připojené zařízení bezpečné pro vaši síť či jiná vaše zařízení, upravte v nastavení routeru přístup k síti pro dané zařízení nebo změňte heslo do vaší sítě.

Ochrana – Pro zajištění ochrany před útoky a škodlivým softwarem doporučujeme instalaci bezpečnostního produktu na vašem zařízení. Vždy dbejte na to, aby byl operační systém a software aktualizovaný. Abyste zůstali chráněni, nikdy se nepřipojujte k nezabezpečené Wi-Fi síti.

✓ [Toto zařízení](#)

Toto zařízení představuje váš počítač v síti.

Síťové adaptéry – Zobrazuje informace o [síťových adaptérech](#).

Oznámení | Strážce sítě

V této kapitole uvádíme seznam oznámení, které může produkt ESET Smart Security Premium zobrazit při detekci některé ze zranitelností ve vašem routeru. U každého oznámení je uveden krátký popis společně s možným řešením nebo kroky po jejichž provedení minimalizujete bezpečnostní riziko u vašeho routeru. Pokud si nejste vědomi úprav v nastavení routeru, doporučujeme vám kontaktovat jeho výrobce nebo svého poskytovatele internetových služeb.

Nalezena potenciální zranitelnost

Váš router možná obsahuje známé zranitelnosti, které lze snadno využít pro průnik do vaší sítě. Aktualizujte firmware ve svém routeru.

Nalezena zranitelnost

Váš router obsahuje známé zranitelnosti, které lze snadno využít pro průnik do vaší sítě. Aktualizujte firmware ve svém routeru.

Nalezena hrozba

Váš router je infikován škodlivým kódem. Restartujte svůj router a proveďte kontrolu znovu.

Administrace vašeho routeru je zabezpečena slabým heslem

Heslo pro přístup do administrace vašeho routeru je slabé a může jej kdokoli uhodnout. Změňte heslo pro přístup do svého routeru.

Nežádoucí síťové přesměrování

Komunikace z vaší sítě směřuje na stránky se škodlivým obsahem. To může znamenat, že byl váš router kompromitován. Změňte nastavení DNS serverů ve svém routeru.

Otevřené síťové služby

Na vašem routeru jsou povoleny citlivé síťové služby, které mohou ostatní zneužít. Může se jednat o chybnou konfiguraci nebo je váš router kompromitován. Zkontrolujte konfiguraci svého routeru.

Otevřené citlivé síťové služby

Na vašem routeru jsou povoleny citlivé síťové služby, které mohou ostatní zneužít. Může se jednat o chybnou konfiguraci nebo je váš router kompromitován. Zkontrolujte konfiguraci svého routeru.

Firmware v routeru není aktuální

Firmware ve vašem routeru je zastaralý a může obsahovat zranitelnosti. Aktualizujte firmware ve svém routeru.

Nežádoucí nastavení routeru

DNS Server, který používá váš router, je kompromitován a můžete být přesměrováni na stránky se škodlivým obsahem. To může znamenat, že byl váš router kompromitován. Změňte nastavení DNS serverů ve svém routeru.

Síťové služby

Na vašem routeru běží standardní síťové služby. Jsou důležité pro běh sítě a pravděpodobně je máte bezpečně nastaveny. Zkontrolujte konfiguraci svého routeru.

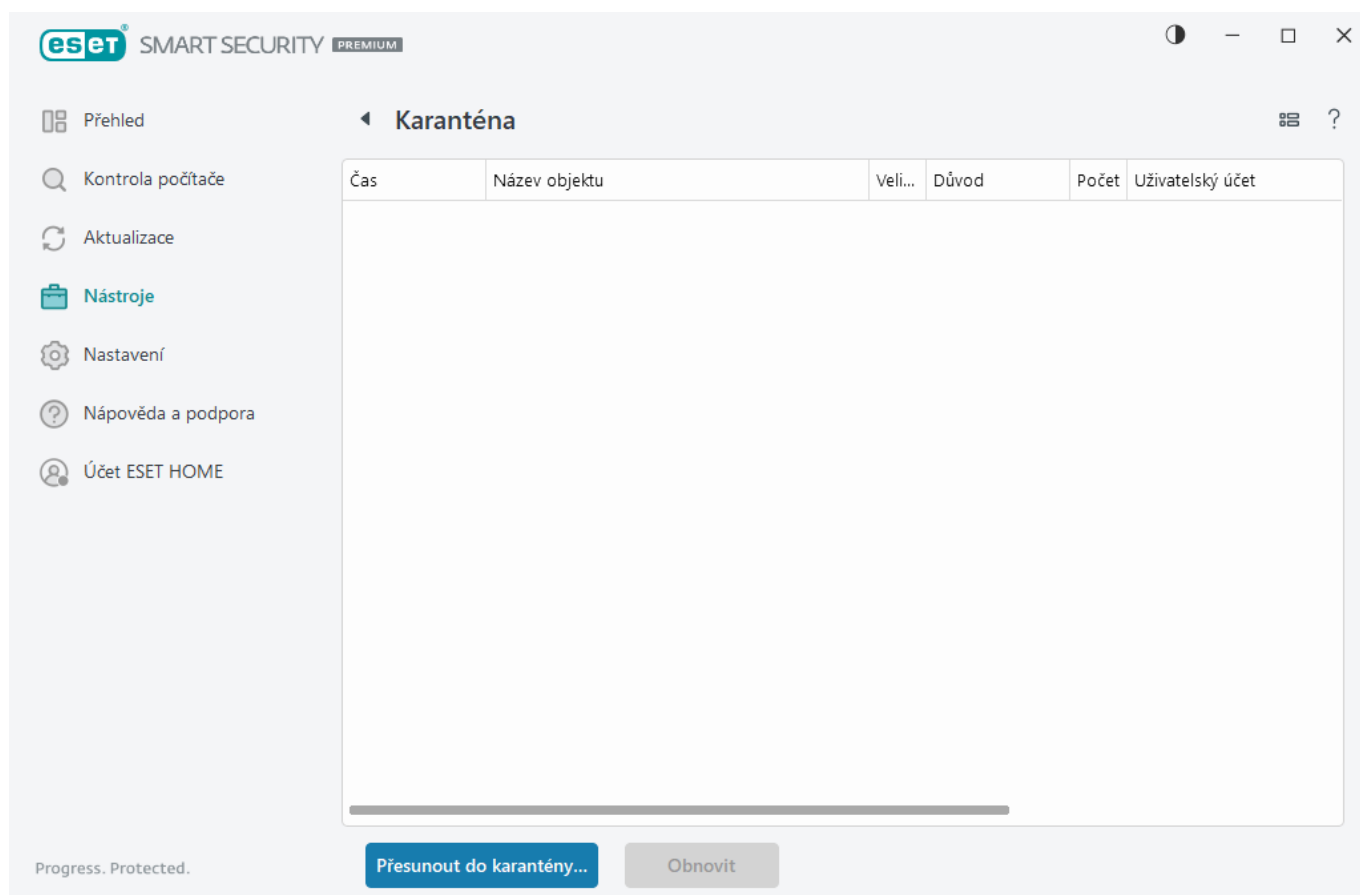
Karanténa

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 Smart Security Premium 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 přidáný uživatelem),
- a počtu detekcí. (např. duplikovanou detekcí stejného souboru, nebo pokud se jedná o archiv obsahující více infiltrací).



Vložení objektu do karantény

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

Soubory mohou být umístěny do karantény, pokud:

- nemohou být léčeny,
- pokud není bezpečné a doporučené jejich odstranění,
- pokud byly ESET Smart Security Premium falešně detekovány,
- nebo pokud soubor vykazuje podezřelou aktivitu, ale není detekován [Ochranami](#).

Pro uložení souboru do karantény máte několik možností:

- Přetáhněte ji způsobem Drag and drop (nakliknout na soubor levým tlačítkem myši, podržet levé tlačítko,

přesunout do zvýrazněné oblasti a tlačítko pustit). Po přesunutí souboru se okno aplikace přesune do popředí.

b. Klikněte na soubor pravým tlačítkem myši a v zobrazeném kontextovém menu vyberte možnost **Rozšířená nastavení > Přesunout soubor do karantény**.

c. V hlavním menu programu přejděte do sekce **Karanténa** a klikněte na tlačítko **Přesunout do karantény...**

d. 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**. Pokud chcete vybrat a odstranit všechny položky v karanténě, můžete stisknout klávesy **Ctrl + A** a poté **Delete**. 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**.

Popis detekce...

Po kliknutí pravým tlačítkem myši na položku a výběrem **Popis detekce** budete přesměrováni do ESET Encyklopedie hrozeb, kde naleznete informace o jednotlivých hrozbách.

Názorné ukázky

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



- [Obnovení objektu z karantény v ESET Smart Security Premium](#)
- [Odstranění objektu z karantény v ESET Smart Security Premium](#)
- [Program ESET mě upozornil na detekci. Co mám dělat?](#)

Soubor se nepodařilo přesunout do karantény

Níže uvádíme důvody, proč není možné některé soubory umístit do karantény:

- **Nemáte oprávnění pro čtení** – to znamená, že si nemůžete zobrazit obsah souboru.
- **Nemáte oprávnění pro zápis** – to znamená, že si nemůžete modifikovat obsah souboru, například přidat do něj nový obsah nebo z něj naopak něco odstranit.
- **Soubor, který se pokoušíte přesunout do karantény je příliš velký** – snižte velikost souboru.

Pokud se vám zobrazí chybová zpráva "Soubor se nepodařilo přesunout do karantény", klikněte na možnost **Více informací**. Následně se zobrazí dialogové okno se seznamem souborů společně s důvodem, proč se jej nepodařilo přesunout do karantény.

Odeslání vzorku k analýze

V případě, že máte v zařízení soubor s podezřelým chováním nebo jste narazili na internetu na podezřelou webovou stránku, můžete je odeslat na analýzu do ESET Research Lab (tato funkce nemusí být k dispozici, závisí na konfiguraci ESET LiveGrid®).

Před odesláním vzorku do společnosti ESET

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, odkud jste obdrželi odkaz, screenshot apod.)

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

1. Odešlete vzorek prostřednictvím formuláře v produktu. Formulář naleznete v hlavním okně produktu na záložce **Nástroje > Odeslat soubor k analýze**. Maximální velikost souboru, který je možné odeslat, je 256 MB.
2. Případně můžete soubor zaslat e-mailem. Pokud dáváte přednost této možnosti, prosím dbejte na to, abyste soubor přidali do archivu WinRAR/WinZIP a ochránili archiv heslem "infected" předtím, než jej odešlete na adresu samples@eset.com.
3. Další informace o nahlášení spamu, falešných detekcí spamu nebo webových stránek nesprávně zařazených modulem Rodičovská kontrola naleznete v článku v [Databázi znalostí ESET](#).

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 detekovaná stránka](#)
- [Falešně detekovaný soubor](#) (soubor detekovaný jako infikovaný není infikovaný)

- [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**.

Pravděpodobně neobdržíte žádnou zpětnou vazbu

i 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) – zadejte původ souboru (zdroj) a jakým způsobem jste k souboru přišli.

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

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

Podezřelá stránka

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

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

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

Falešně detekovaný soubor

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

obsažené v detekčním jádru.

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

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

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

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

i 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.

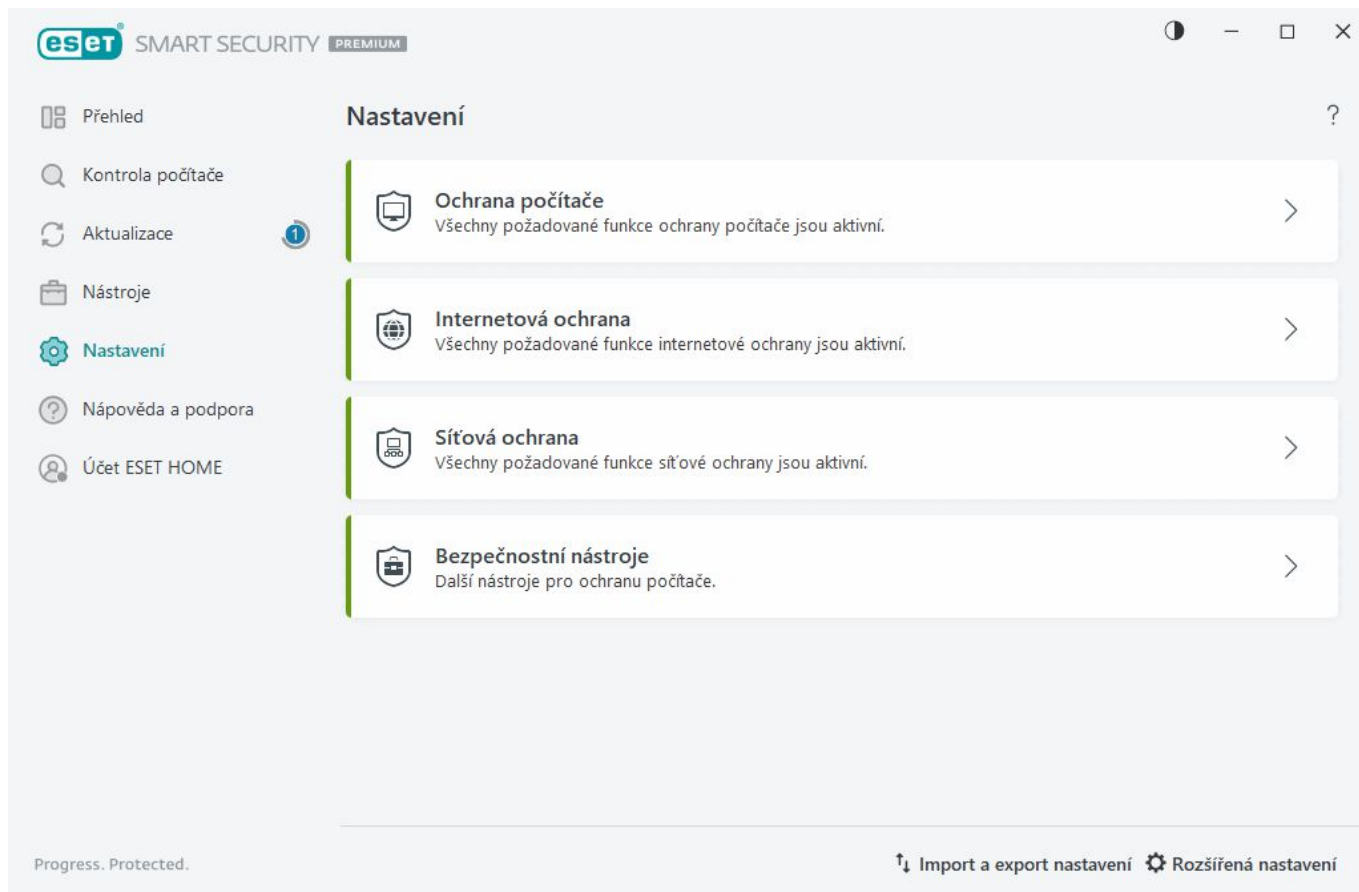
Ostatní

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.

Nastavení

Dostupné ochranné funkce najdete v [hlavním okně programu](#) > **Nastavení**.



Záložka **Nastavení** je rozdělena do následujících skupin:

 [Ochrana počítače](#)

 [Internetová ochrana](#)

 [Síťová ochrana](#)

 [Bezpečnostní nástroje](#)

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

Ochrana počítače

Kliknutím na položku **Ochrana počítače** v [hlavním okně programu](#) > **Nastavení** zobrazíte přehled všech modulů ochrany:

- [Rezidentní ochrana souborového systému](#) – všechny soubory jsou kontrolovány v momentu, kdy je vytvoříte, otevřete nebo spustíte.
- [ESET LiveGuard](#) je funkce, která přidává vrstvu cloudové ochrany speciálně navrženou pro snížení dopadu zcela nových hrozeb


- Proaktivní ochrana – blokuje spouštění nových souborů až do obdržení výsledku analýzy ESET LiveGuard. Chcete-li odblokovat analyzovaný soubor, klikněte na něj pravým tlačítkem myši a vyberte možnost **Odblokovat soubor analyzovaný prostřednictvím ESET LiveGuard**.


- [Správa zařízení](#) – pomocí této součásti můžete uživatelům nastavovat, kontrolovat nebo blokovat přístupy k výměnným médiím (CD/DVD/USB aj.).


- [Host Intrusion Prevention System \(HIPS\)](#) – systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně na základě přizpůsobené sady pravidel.

- [Herní režim](#) – po aktivaci Herního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. Obdržíte varovnou zprávu o potenciální bezpečnostní hrozbě a hlavní okno se zbarví do oranžova.

- [Ochrana webkamery](#) – kontroluje procesy a aplikace, které mají přístup k webkameře.


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

 Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.

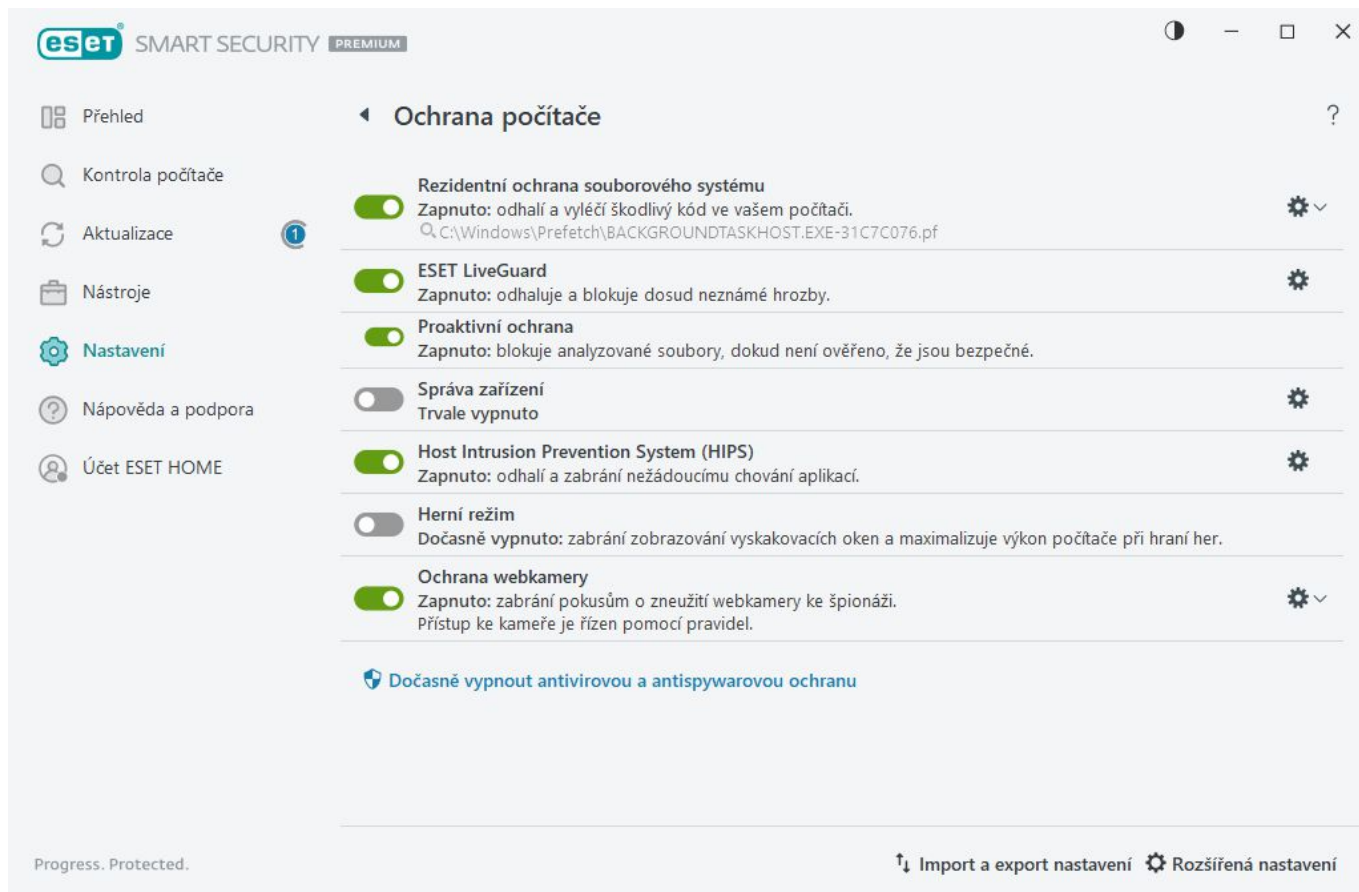
Kliknutím na ikonu ozubeného kola  na řádku s modulem ochrany přejdete do jeho rozšířených nastavení.

Pro nastavení **Rezidentní ochrany souborového systému** klikněte na  a vyberte si z následujících možností:

- **Nastavit...** – po kliknutí se zobrazí [rozšířená nastavení Rezidentní ochrany souborového systému](#).
- **Upravit výjimky** – kliknutím si zobrazíte dialogové okno pro [nastavení detekčních výjimek](#), pomocí kterého můžete vyloučit soubory a složky z kontroly.

Pro nastavení **Ochrany webkamery** klikněte na  a vyberte si z následujících možností:

- **Nastavit...** – otevře [rozšířená nastavení Ochrany webkamery](#).
- **Blokovat do restartu veškerý přístup** – zablokuje přístup ke kameře až do restartu nebo nového zapnutí zařízení,
- **Blokovat trvale veškerý přístup** – zablokuje přístup ke kameře až do odblokování, které provedete ručně,
- **Odblokovat přístup** – touto možností odblokujete přístup ke kameře. Tato možnost se zobrazí jen v případě, kdy je přístup blokován.



Dočasně vypnout antivirovou a antispywarovou ochranu – pomocí této možnosti vypnete všechny moduly antivirové a antispywarové ochrany. Po kliknutí se zobrazí dialogové okno, ve kterém můžete vybrat z rozbalovacího menu **časový interval**, po který bude rezidentní ochrana vypnuta. Klikněte na Použít pro potvrzení.

Nalezena infiltrace

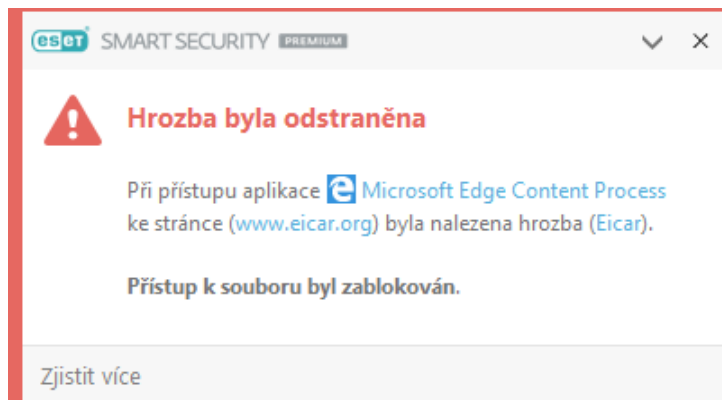
Infiltrace se mohou do počítače dostat z různých zdrojů: z [webových stránek](#), ze sdílených složek, prostřednictvím e-mailu, z [výměnných médií](#) (USB, externí disků, CD a DVD jiných).

Standardní chování

ESET Smart Security Premium 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 [Úrovně léčení](#).



Kontrola počítače na výskyt infikovaných souborů

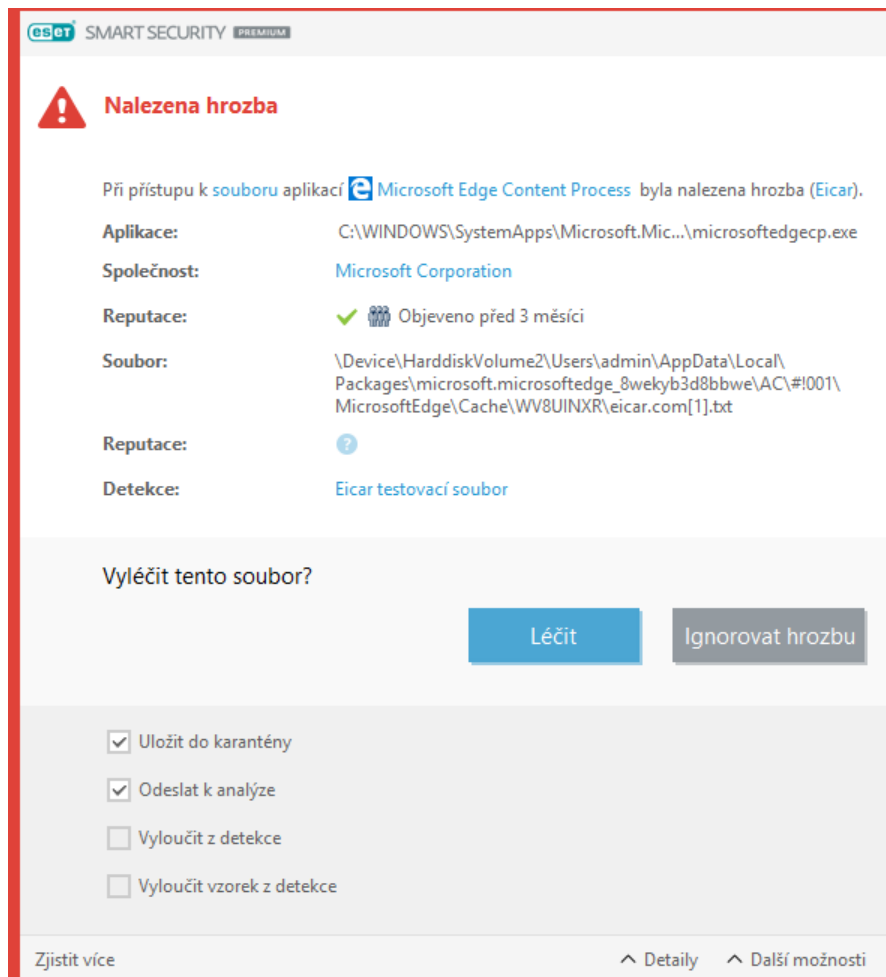
Pokud se váš počítač chová podezřele nebo máte podezření, že je infikován (zamrzá, je pomalý atp.), postupujte podle následujících kroků:

1. Otevřete ESET Smart Security Premium a přejděte na záložku **Kontrola počítače**.
2. Klikněte na **Provést kontrolu počítače** (bližší informace naleznete v kapitole [Kontrola počítače](#)).
3. Po dokončení kontroly, zkontrolujte zobrazený protokol.

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

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 nevléčena. 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 Smart Security Premium 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. Vyberte akci, kterou chcete provést (akce se nastavuje individuálně pro každý soubor ze seznamu) a klikněte na **Dokončit**.

Mazání souborů v archivech

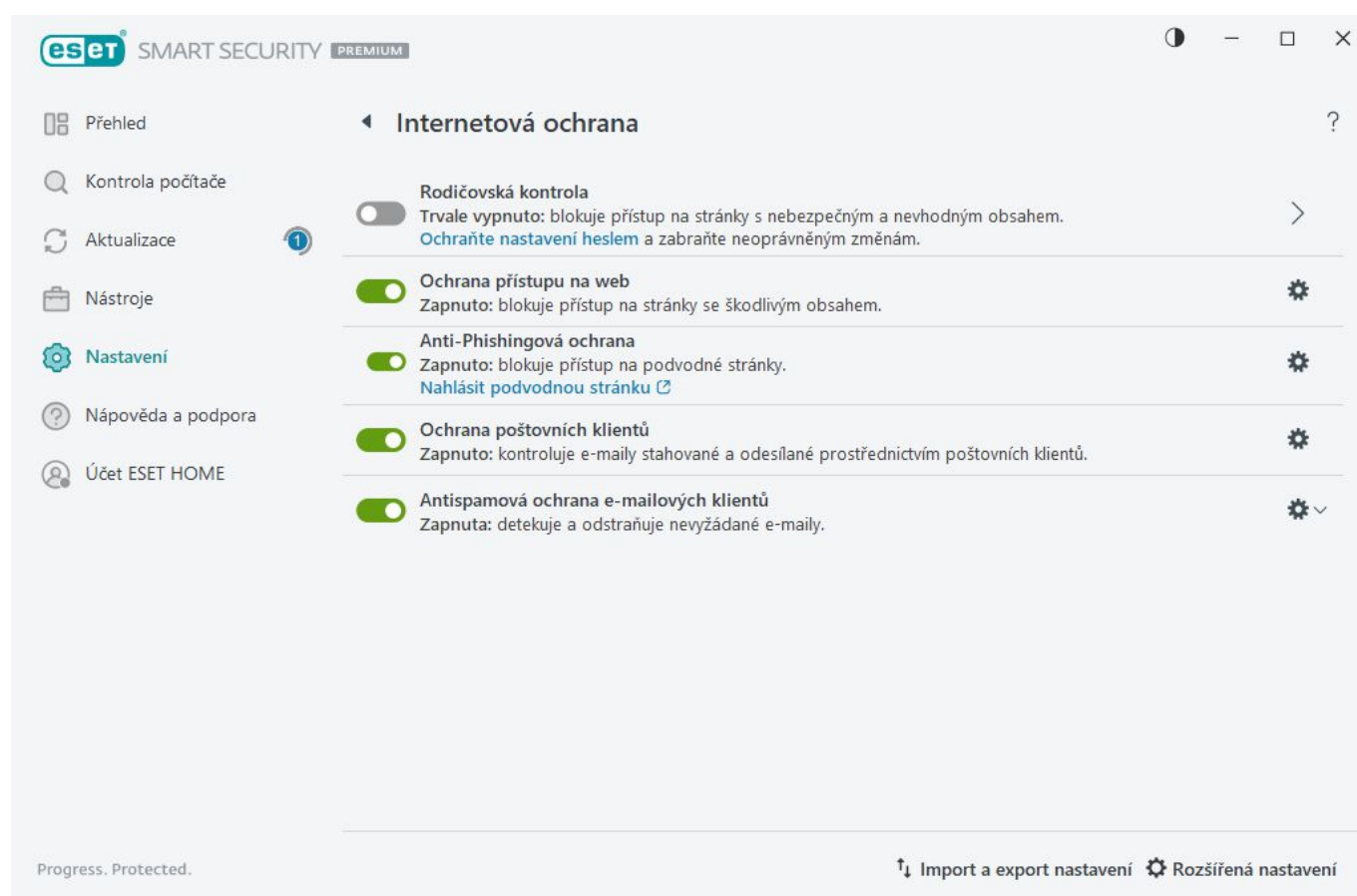
Pokud je zjištěna infiltrace uvnitř archivu, bude archiv při standardní úrovni léčení odstraněn pouze v případě, že obsahuje pouze infikovaný soubor. Archiv nebude vymazán, pokud kromě infiltrace obsahuje také nezávadné soubory. Opatrnost je potřeba dodržovat při nastavení přísné úrovně léčení, kdy v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


Internetová ochrana

Internetové připojení se stalo u počítačů standardem. Bohužel i pro šíření škodlivého kódu. Otevřete [hlavní okno programu](#) > **Nastavení** > **Internetová ochrana** a nakonfigurujte funkce na ESET Smart Security Premium, které zvyšují internetovou ochranu.

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

 Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.



Kliknutím na ikonu ozubeného kola  vedle modulu ochrany získáte přístup k pokročilým nastavením tohoto modulu.

Rodičovská kontrola – modul [Rodičovská kontrola](#) zabrání vašim dětem v přístupu na nevhodné nebo závadné stránky na internetu.

[Ochrana přístupu na web](#) kontroluje komunikaci HTTP/HTTPS na přítomnost škodlivého kódu a phishingu. Ochrana přístupu na web by měla být vypnuta pouze pro účely řešení problémů.

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

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



Předtím, než odešlete stránku do společnosti ESET, se ujistěte, že splňuje alespoň jedno z níže uvedených kritérií:

- Stránka není detekována jako škodlivá.
- Stránka je chybně detekována jako škodlivá. V tomto případě [nehlaste neoprávněně blokovanou stránku](#).

[Ochrana poštovních klientů](#) zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3(S) a IMAP(S). Zásuvný modul pro e-mailového klienta umožňuje ESET Smart Security Premium ovládat veškerou komunikaci z/do e-mailového klienta.

[Antispamová ochrana poštovních klientů](#) filtruje nevyžádané e-mailové zprávy.

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

- **Nastavit** – kliknutím si otevřete [rozšířená nastavení antispamové ochrany poštovních klientů](#).
- **Uživatelský seznam adres** (pokud je povolen) – kliknutím si otevřete [dialogové okno](#), ve kterém můžete definovat pravidla antispamu. Pravidla definovaná v tomto seznamu jsou platná pro aktuálně přihlášeného uživatele.
- **Globální seznam adres** (pokud je povolen) – kliknutím si otevřete [dialogové okno](#), ve kterém můžete definovat pravidla antispamu. Pravidla definovaná v tomto seznamu se aplikují na všechny uživatele.

Anti-Phishingová ochrana

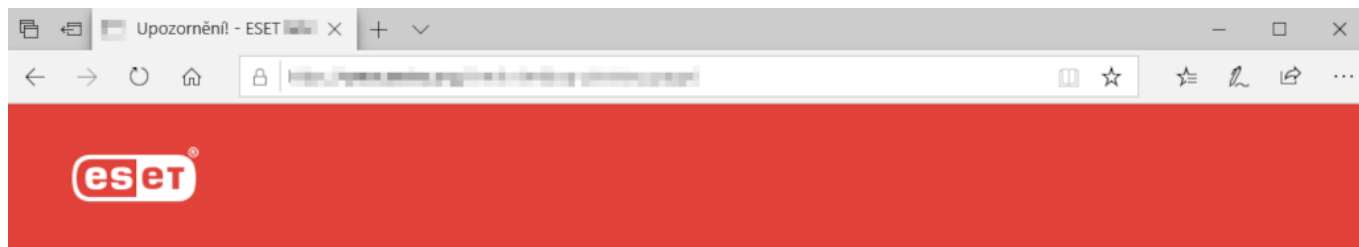
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem útočníků využívajících phishing je získání citlivých dat, jako jsou čísla bankovních účtů, PIN kódy a další. Více informací naleznete v [glosáři](#). ESET Smart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

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

Podrobnější informace o fungování Anti-Phishingové ochrany ESET Smart Security Premium 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).



Potenciální pokus o phishing

Stránka se pokouší z návštěvníků získat osobní a citlivé informace jako jsou přihlašovací údaje, čísla bankovních karet atp.

Chcete se vrátit na předchozí stránku?

Přejít zpět

Ignorovat hrozbu

[Nahlásit nesprávně blokovanou stránku](#)

[Více informací o phishingu](#) | www.eset.cz



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

Nahlásit podvodnou stránku

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

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

Rodičovská kontrola


V sekci Rodičovská kontrola můžete konfigurovat nastavení modulu, které pomůže chránit vaše děti a nastavit omezení pro používání zařízení a služeb. Cílem je zabránit dětem, dospívajícím a zaměstnancům přístup na stránky

s nevhodným nebo škodlivým obsahem.

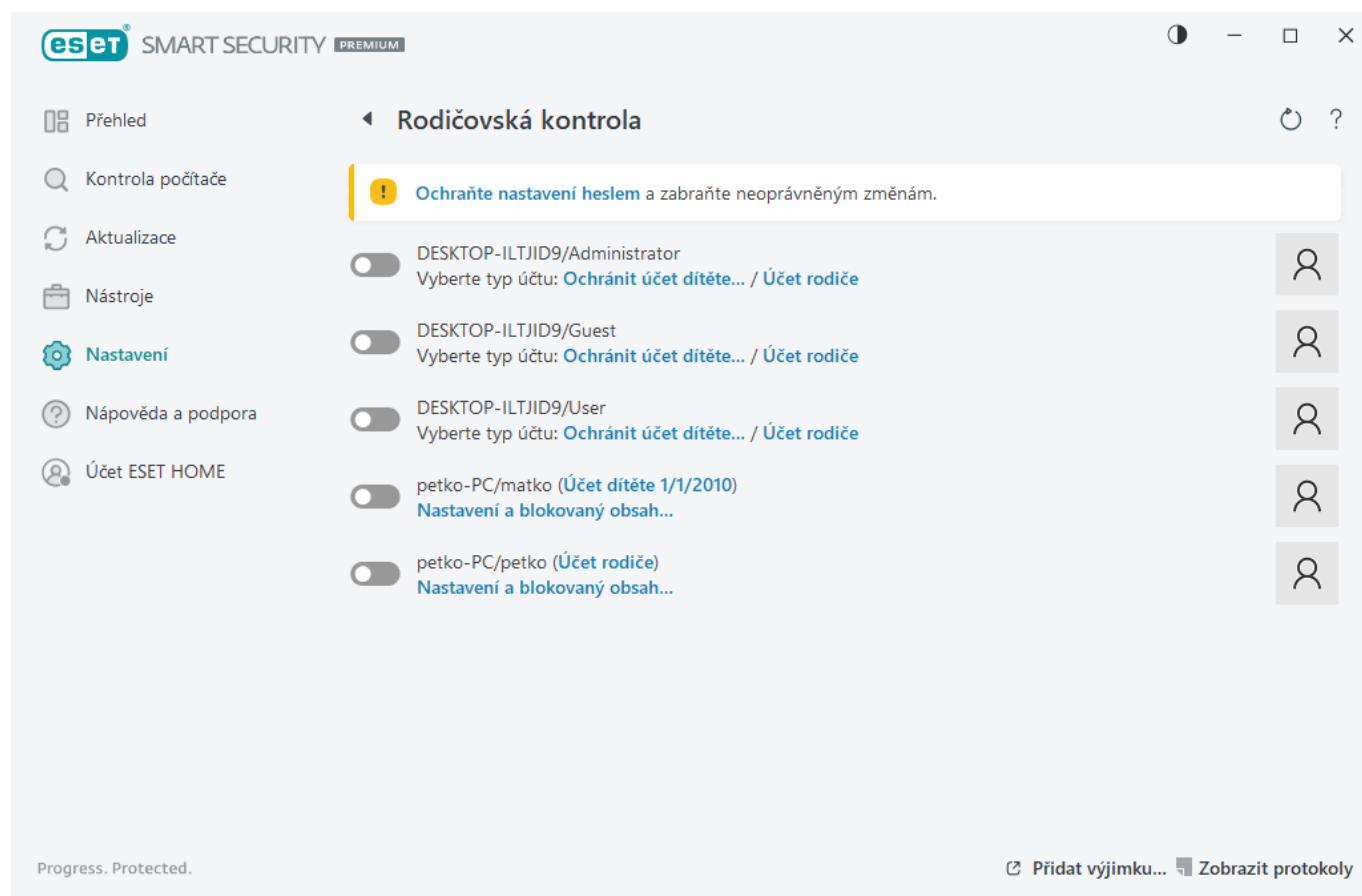
Rodičovská kontrola umožňuje blokovat webové stránky, které mohou obsahovat nevhodný obsah. Kromě toho jako rodiče můžete zakázat přístup na 40 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

K aktivaci Rodičovské kontroly ve vybraném uživatelském účtu postupujte dle následujících kroků:

1. Ve výchozím nastavení ESET Smart Security Premium je Rodičovská kontrola vypnuta. Zapnout ji můžete dvěma způsoby:



- V [hlavním okně programu](#) přejděte na záložku **Nastavení > Internetová ochrana** a pomocí přepínače  aktivujte **Rodičovskou kontrolu**.
- Otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana přístupu na web** > **Rodičovská kontrola** a poté pomocí přepínače **zapněte rodičovskou kontrolu**.

2. V [hlavním okně programu](#) přejděte na záložku **Nastavení > Bezpečnostní nástroje > Rodičovská kontrola**. Přestože je funkce **Rodičovské kontroly** **zapnuta**, je nutné definovat uživatelské účty, pro které se má použít. Klikněte na symbol šipky a dále na možnost **Ochránit účet dítěte**. V následujícím okně vyberte věk, který odpovídá danému uživateli, podle něhož se stanovuje úroveň filtrování webových stránek. Nyní bude rodičovská kontrola pro vybraný uživatelský účet kompletně nastavená a zapnutá. Dále klikněte na možnost **Nastavení a blokový obsah...** pod jménem účtu k úpravě kategorií, které chcete povolit nebo blokovat v tabulce [Kategorií](#). Pro blokování nebo povolení konkrétních stránek přejděte na záložku [Výjimky](#).




Na záložce ESET Smart Security Premium **Nastavení > Internetová ochrana > Rodičovská kontrola** jsou dostupné tyto možnosti:

Účty uživatelů Windows

Pokud jste vytvořili roli pro existující účet, bude zobrazena právě zde. Vedle nabídky Rodičovská kontrola klikněte na přepínač  tak, aby se zbarvil dozelena . Pod aktivním účtem najdete možnost [Nastavení a blokování obsahu...](#), která slouží pro konfiguraci seznamu povolených kategorií, blokováných a povolených stránek.

Odkazy v dolní části okna obsahují


Přidat výjimku... – po kliknutí přidáte snadno a rychle stránku, kterou chcete povolit nebo naopak blokovat.

Zobrazit protokoly – zobrazí podrobný protokol o činnosti rodičovské kontroly (blokování stránek, účet, kterému byla stránka zablokovaná, důvod zablokování, atd.). Tento protokol můžete filtrovat na základě nastavených kritérií kliknutím na **Filtrování** .

Rodičovská kontrola

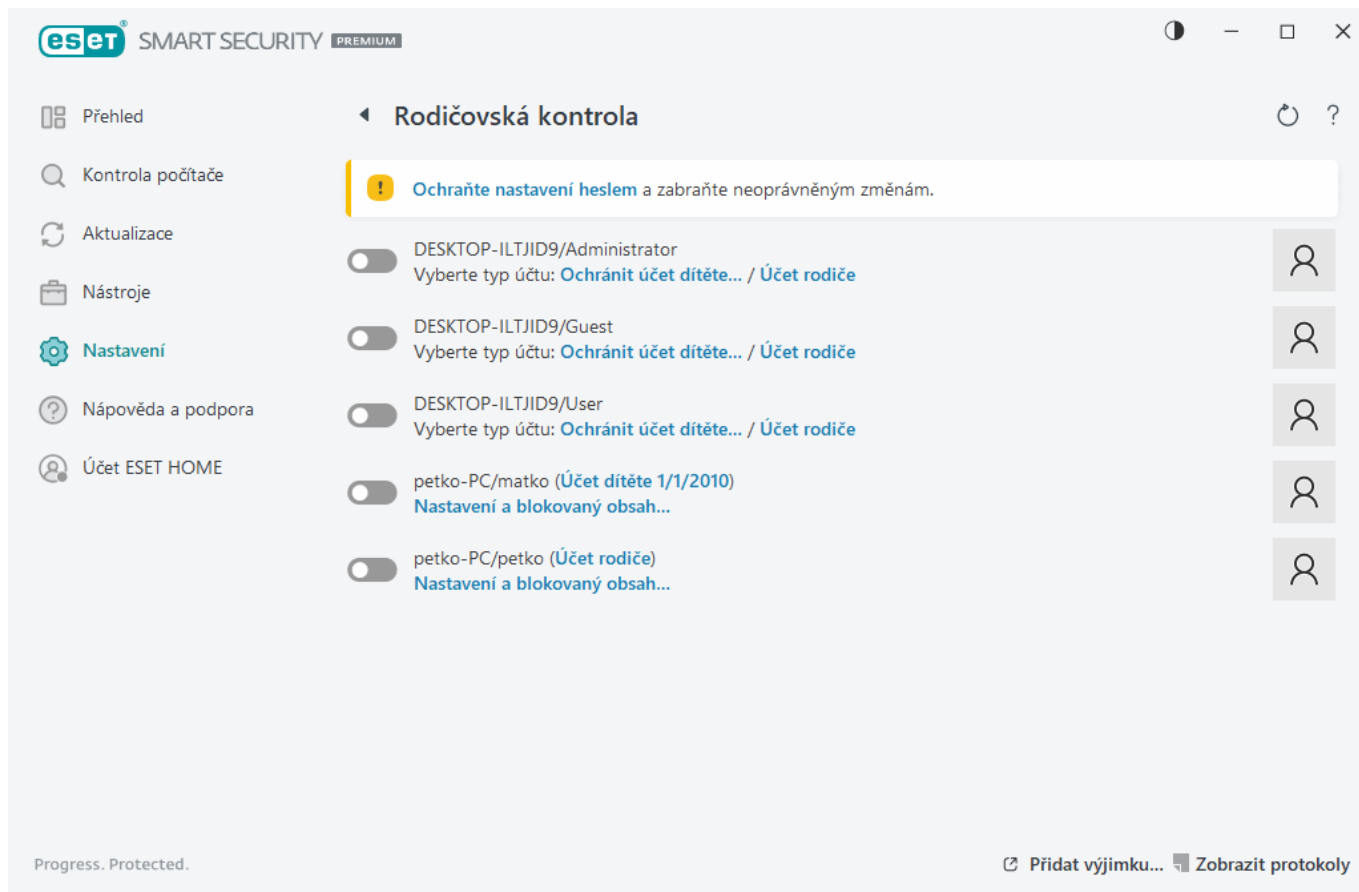
Při kliknutí na přepínač k vypnutí Rodičovské kontroly se zobrazí okno s otázkou **Vypnout rodičovskou kontrolu?** Nastavte čas, na jak dlouho chcete kontrolu vypnout. V závislosti na výběru se kontrola **dočasně** nebo **trvale** vypne.



Důležité je, abyste si nastavení ESET Smart Security Premium ochránili heslem. Heslo nastavíte v části [Přístup k nastavení](#). Pokud není nastaveno žádné heslo pro ochranu nastavení, na hlavní obrazovce programu se zobrazí doporučení **Nastavit heslo pro ochranu nastavení**. Mějte na paměti, že omezení rodičovskou kontrolou se aplikuje pouze na uživatelský účet se standardním oprávněním. Účet s právem Administrátor může nastavení kdykoli obejít.

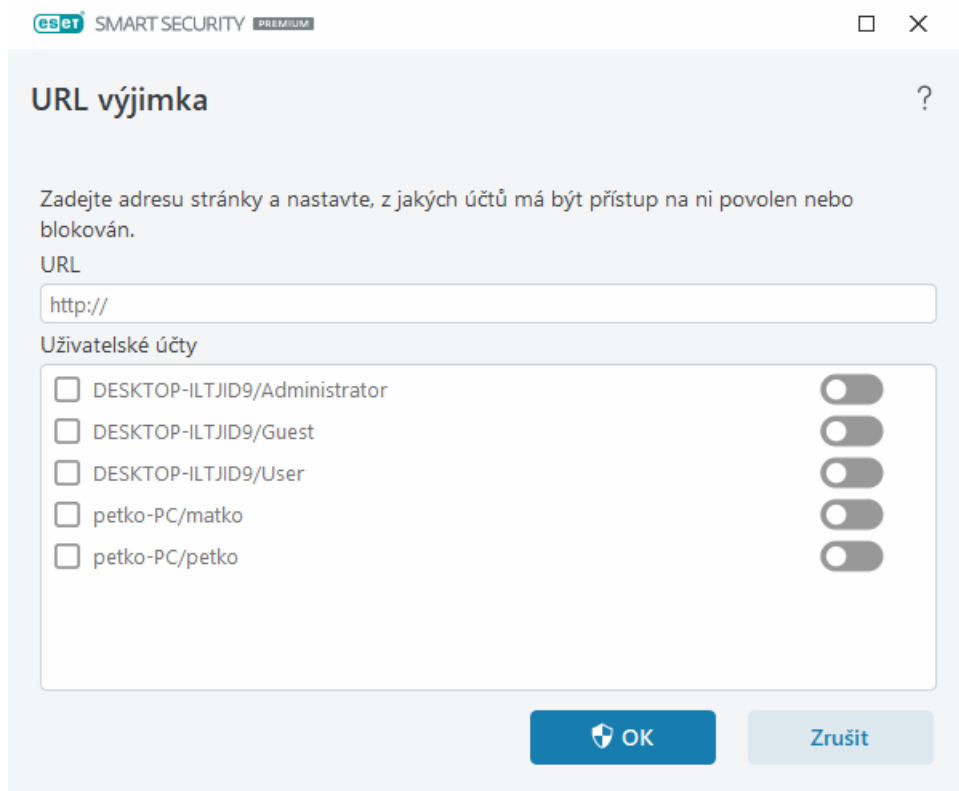
 Rodičovská kontrola vyžaduje pro správnou funkci zapnutou [Kontrolu síťové komunikace](#), [Kontrolu HTTP\(S\) komunikace](#) a [Firewall](#). Všechny tyto funkce jsou standardně zapnuté.

Výjimky pro webové stránky

Pro vytvoření výjimky pro webovou stránku přejděte v hlavním menu na záložku **Nastavení > Internetová ochrana > Rodičovská kontrola** a klikněte na možnost **Přidat výjimku...** v dolní části okna.

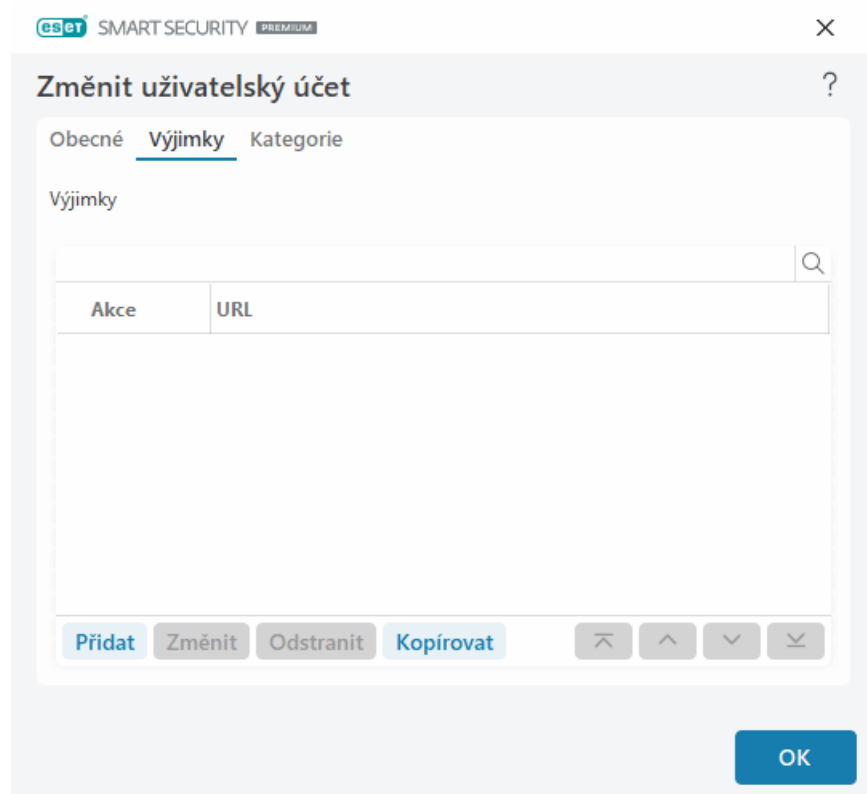


V zobrazeném dialogovém okně zadejte **URL** a dále u každého uživatelského klikněte na ikonu  nebo  – v závislosti na tom, zda chcete uživateli přístup na stránku povolit nebo zakázat. Akci dokončete kliknutím na tlačítko **OK**.



Pro vymazání URL adresy ze seznamu klikněte na **Nastavení > Internetová ochrana > Rodičovská kontrola**, klikněte na **Nastavení a blokový obsah** pod názvem účtu uživatele, který chcete měnit. Následně v okně

vyberte záložku **Výjimky**, klikněte na adresu ze seznamu a poté na tlačítko **Odstranit** pod seznamem.



V seznamech URL adres není možné používat zástupné znaky ** (hvězdička) a ? (otazník). Adresy s více TLD je nutné zadat ručně (*examplepage.com*, *examplepage.sk*, ...). Pokud vložíte adresu domény do seznamu, veškerý obsah nacházející se na této doméně a všechny její subdomény (například *sub.examplepage.com*) budou blokovány nebo povoleny na základě definované akce.

i Blokování nebo povolení specifické internetové stránky může být přesnější než blokování nebo povolení celé kategorie internetových stránek. Při změně těchto nastavení buďte opatrní.

Kopírovat výjimky z účtu

Pomocí kontextového menu můžete zkopírovat výjimky vytvořené pro již existující uživatelský účet a tím si usnadnit konfiguraci nového uživatelského účtu.


Kopírovat kategorie z účtu

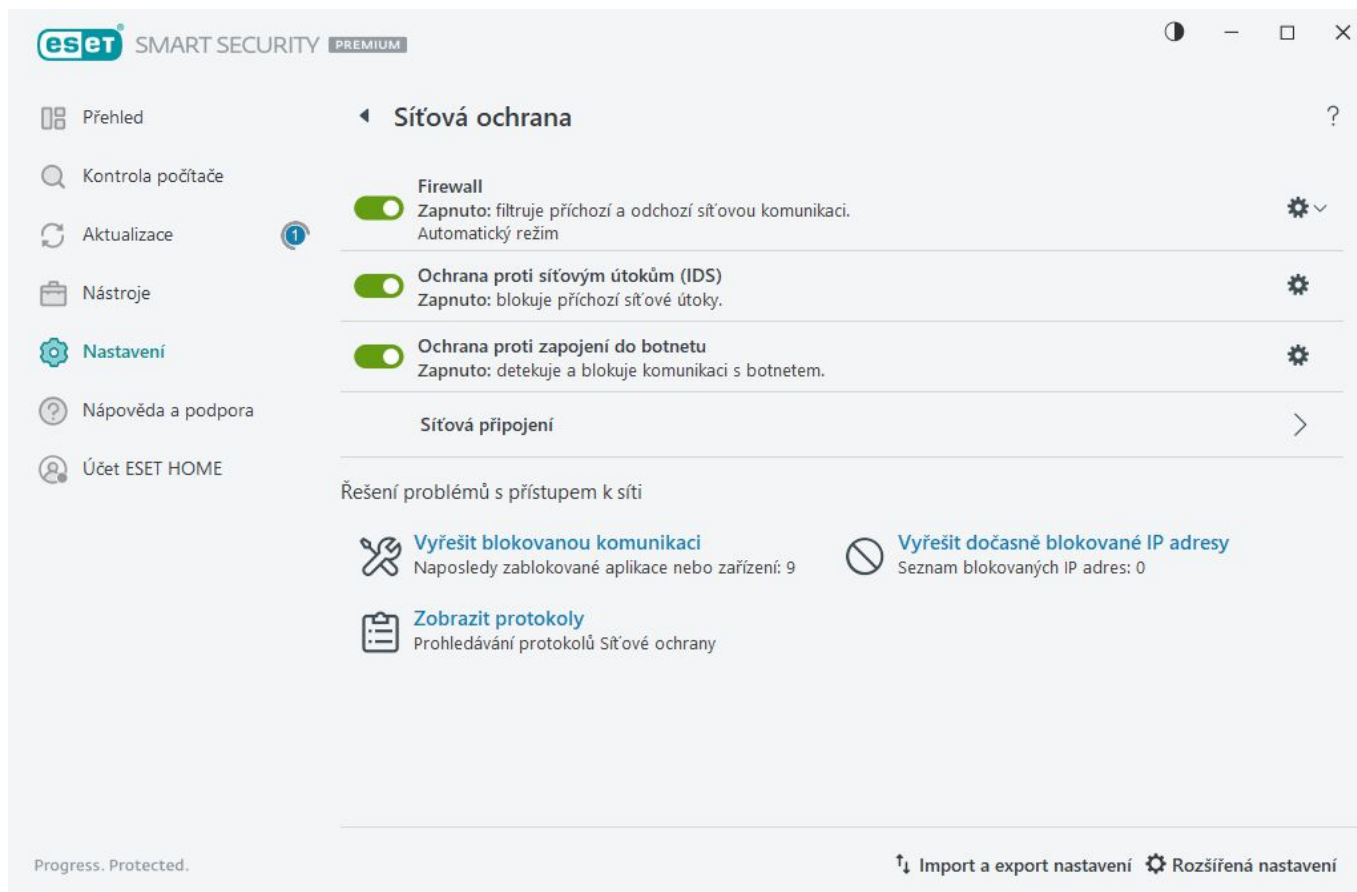
Umožňuje zkopírovat seznam blokových nebo povolených kategorií z existujícího upraveného účtu.


Síťová ochrana

Otevřete [hlavní okno programu](#) > **Nastavení** > **Síťová ochrana** a nakonfigurujte základní nastavení síťové ochrany nebo vyřešte problémy se síťovou komunikací.

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

 Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.



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

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

Nastavit... – otevřou se [Rozšířená nastavení firewallu](#), kde můžete nastavit, jak bude firewall zpracovávat síťovou komunikaci.

Dočasně vypnout firewall – filtrování komunikace firewallem úplně vypnuto a všechna příchozí i odchozí spojení jsou povolena. Pokud je filtrování síťové komunikace firewallem vypnuté, obnovíte jej kliknutím na **Zapnout firewall**.

Blokovat veškerou komunikaci – každá příchozí a odchozí komunikace je firewallem bez upozornění uživatele zablokována. Použití této možnosti je vhodné při podezření na možná kritická bezpečnostní rizika, která vyžadují odpojení systému od sítě. Pokud je **komunikace zablokována**, obnovíte ji po kliknutí na **Povolit veškerou komunikaci**.

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

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

[Ochrana proti síťovým útokům \(IDS\)](#) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Komunikace vyhodnocená jako škodlivá, bude blokována. Zároveň vás ESET Smart Security Premium upozorní na případy, kdy se připojujete k nezabezpečené nebo slabě zabezpečené bezdrátové síti.

Ochrana proti zapojení do botnetu – Rychle a efektivně zaměří škodlivý kód ve vašem systému.

[Síťová připojení](#) – zobrazí informace o sítích, ke kterým jsou připojeny síťové adaptéry.

Vyřešit blokovanou komunikaci – pomůže vám vyřešit problémy s připojením způsobené Firewalllem. Pro více informací přejděte do kapitoly [Průvodce řešením problémů](#).


Vyřešit dočasně blokové IP adresy – zobrazí [seznam IP adres, které byly detekovány jako zdroj útoků a přidány na blacklist](#).

Zobrazit protokoly – otevře [Protokol](#) síťové ochrany.

Síťová spojení

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

Dvojitým kliknutím na připojení v seznamu zobrazíte jeho podrobnosti a podrobnosti o [síťovém adaptéru](#).

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

- **Změnit** – otevře okno [Nastavení síťové ochrany](#), kde můžete přiřadit [profil síťové ochrany](#) konkrétní síti
- **Zapomenout** – obnoví výchozí konfiguraci síťového připojení
- **Zkontrolovat síť prostřednictvím Strážce sítě** – otevře [Strážce sítě](#) ke spuštění kontroly sítě
- **Označit jako "Moje síť"** – přidá k síti štítek "Moje síť"; tato značka se zobrazí vedle sítě v celém ESET Smart Security Premium pro lepší identifikaci a přehled o zabezpečení
- **Zrušit označení "Moje síť"** – odstraní označení "Moje síť", ale pouze v případě, že síť je již označena

Detaily síťového připojení

Dvojitým kliknutím na připojení v seznamu [Síťová připojení](#) zobrazíte jeho podrobnosti spolu s podrobnostmi o síťovém adaptéru. Podrobnosti o síťovém připojení a adaptéru vám pomohou identifikovat síť, kterou se snažíte nakonfigurovat v sekci [Ochrana síťového připojení](#).

Detaily síťového připojení:

- Stav síťového připojení
- Datum a čas první detekce sítě
- Kdy byla síť naposledy aktivní
- Celková doba připojení k této síti
- [Profil síťového připojení](#)
- Profil síťového připojení nastavený v systému Windows

- [Konfigurace síťové ochrany](#) (zda je síť důvěryhodná)

Podrobnosti o síťovém adaptéru:

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

Řešení problémů s přístupem k síti

Tento průvodce vám pomůže při řešení problémů s připojením způsobených firewallem. **Řešení problémů s přístupem k síti** najdete v [hlavním okně programu](#) > **Nastavení** > **Síťová ochrana** > **Vyřešit blokovanou komunikaci**.

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

Nejprve z rozbalovacího menu vyberte časové období, ve kterém byla komunikace zablokována. Seznam nedávno zablokovaných komunikací poskytuje přehled o typu aplikace nebo zařízení, jejich reputaci a celkovém počtu aplikací a zařízení zablokovaných v daném časovém období. 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 blokové komunikace. Pokud se i nadále objevují problémy s aplikací nebo zařízení nefunguje podle očekávání, klikněte na **vytvořit jiné pravidlo** a veškerá komunikace, která byla dříve pro dané zařízení blokována, bude nyní povolena. Některá pravidla se uplatní až při dalším startu systému.

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



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

Seznam dočasně blokových IP adres

Chcete-li zobrazit IP adresy, které byly detekovány jako zdroje útoků a jsou na seznamu dočasně blokových IP adres, otevřete [hlavní okno programu](#) > **Nastavení** > **Síťová ochrana** > **Vyřešit dočasně blokové IP adresy**. 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).

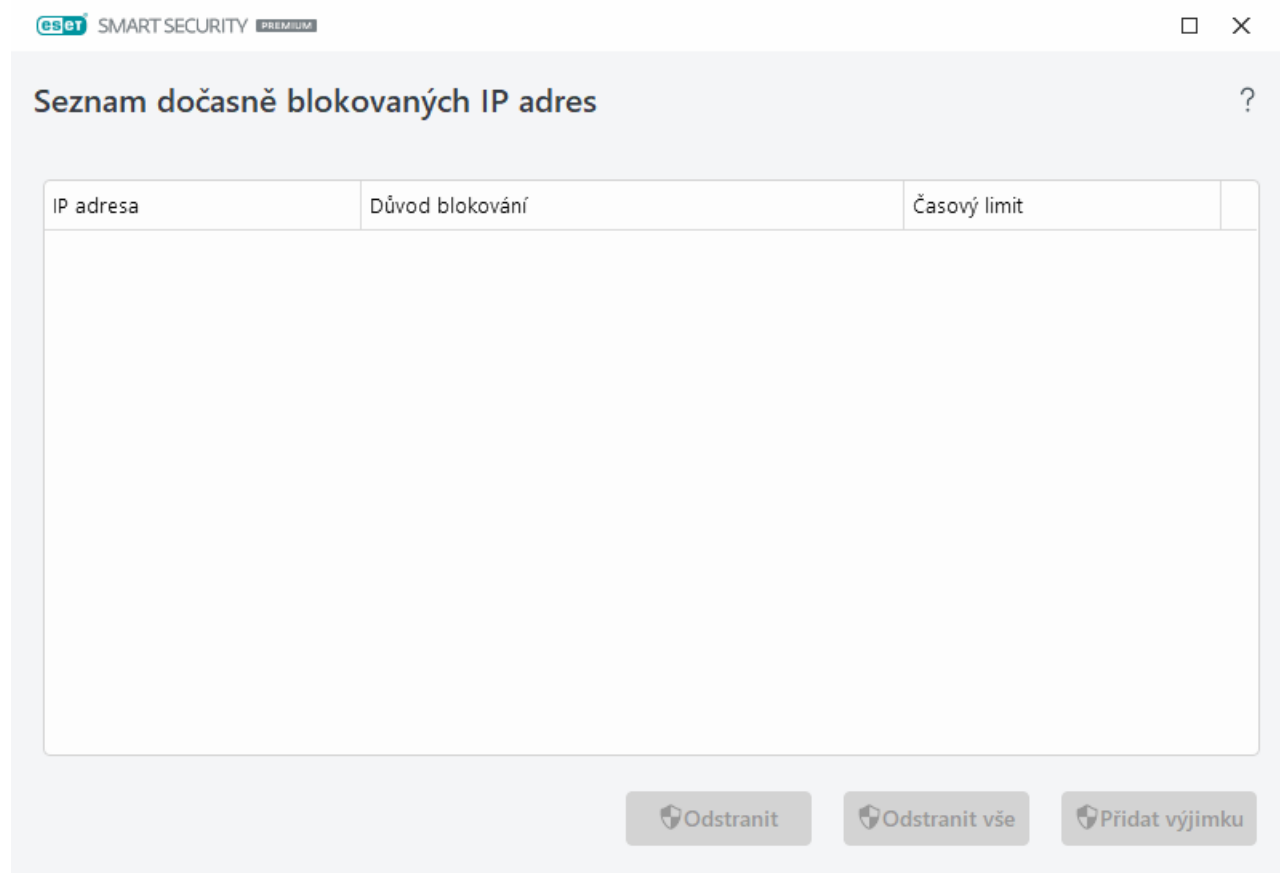
Čas vypršení – doba, na jak dlouho bude komunikace z dané adresy blokována.

Ovládací prvky

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

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

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



Protokoly síťové ochrany

Síťová ochrana ESET Smart Security Premium ukládá důležité události do protokolu. Chcete-li zobrazit soubor protokolu, otevřete [hlavní okno programu](#) > **Nastavení** > **Síťová ochrana** > **Zobrazit protokoly**.

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

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

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

Zneužití zranitelnosti zabezpečení



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

Řešení problémů s firewallem

Pokud se po instalaci ESET Smart Security Premium potýkáte s problémy s připojením k internetu / síťovým prostředkům, existuje několik způsobů jak zjistit, zda problémy s připojením nezpůsobil firewall. Kromě toho vám Firewall pomůže vytvořit nová pravidla nebo výjimky pro řešení problémů s připojením.

V následujících kapitolách naleznete možné řešení problémů způsobených Firewallem:

- [Řešení problémů s přístupem k síti](#)

- [Protokolování a vytváření pravidel nebo výjimek z protokolu](#)
- [Vytváření výjimek z oznámení firewallu](#)
- [Rozšířené protokolování síťové ochrany](#)
- [Řešení problémů s Kontrolou síťové komunikace](#)

Protokolování a vytváření pravidel nebo výjimek z protokolu

Standardně ESET Firewall nezaznamenává všechna zablokovaná spojení. Pro zobrazení, co bylo zablokováno Sítovou ochranou, je nutné zapnout rozšířené protokolování v [Rozšířených nastaveních](#) > **Nástroje** > **Diagnostika** > **Pokročilé protokolování** > **Aktivovat rozšířené protokolování síťové ochrany**. Pokud v protokolu naleznete spojení, které nechcete blokovat, stačí na něj kliknout pravým tlačítkem myši a z kontextového menu vybráním možnosti **Příště neblokovat podobné události** vytvořit IDS pravidlo. Mějte na paměti, že protokol všech zablokovaných spojení může obsahovat stovky záznamů a může být obtížné v něm najít konkrétní spojení. Po vyřešení problému nezapomeňte protokolování opět deaktivovat.

Pro více informací přejděte do kapitoly [Protokoly](#).

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

Vytvoření pravidla z protokolu

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

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

1. V [Rozšířených nastaveních](#) > **Nástroje** > **Protokoly** nastavte **Zaznamenávat události od úrovně na Diagnostické**.
2. Aktivujte možnost **Upozornit na příchozí útoky využívající bezpečnostní zranitelnosti** v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Další možnosti** > **Detekce útoků**.

Vytváření výjimek z oznámení firewallu

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

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

Rozšířené protokolování síťové ochrany

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

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

Řešení problémů s Kontrolou síťové komunikace

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

Problémy s aktualizací nebo zabezpečeným spojením

Pokud se aplikace nedokáže aktualizovat nebo komunikační kanál není zabezpečený:

- Pokud máte aktivní filtrování protokolu [SSL/TLS](#), zkuste je dočasně vypnout. V případě, že to pomůže, ponechte filtrování protokolu SSL/TLS aktivní a vytvořte výjimku pro problematickou komunikaci: Deaktivace SSL/TLS. Znovu proveďte aktualizaci. Zobrazí se dialogové okno s informací o šifrované komunikaci. Ujistěte se, že komunikující aplikace je skutečně ta, která nefunguje, a detailně prozkoumejte certifikát serveru. Následně vyberte možnost zapamatovat akci pro tento certifikát nebo klikněte na tlačítko Ignorovat. Pokud se již nezobrazí žádná další dialogová okna, přepněte režim filtrování zpět na automatický. Tím by měl být problém vyřešen.
- Pokud daná aplikace není prohlížečem nebo e-mailovým klientem, můžete ji zcela vyloučit z [Ochrany přístupu na web](#) (v případě prohlížeče nebo e-mailového klienta byste byli vystaveni nebezpečí). Všechny aplikace, jejichž komunikace již byla v minulosti filtrována, by se měly zobrazit v seznamu aplikací, ve kterém je můžete vyloučit z filtrování protokolů. Ruční zadávání tedy není nutné.

Problémy s přístupem k síti

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

Problémy s konkrétní webovou stránkou

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

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

Pokud máte aktivní SSL/TLS, ESET Smart Security Premium zajistí, aby nainstalované aplikace důvěřovaly způsobu filtrování protokolu SSL tím, že do svého úložiště certifikátů importují certifikát. Některé aplikace mohou pro import certifikátu vyžadovat restart. V tomto případě se jedná o internetový prohlížeč Firefox a Opera. Ujistěte se tedy, že neběží žádný internetový prohlížeč (nejlépe pohledem do Správce úloh, zda se v něm na záložce Procesy nenachází proces firefox.exe, thunderbird.exe nebo opera.exe) a zkuste to znovu.

Neplatný vydavatel nebo podpis certifikátu

V tomto případě se import certifikátu nezdařil. Nejprve se ujistěte, zda cílová aplikace neběží. Pak deaktivujte SSL/TLS a znovu jej aktivujte. Poté by již mělo dojít ke korektnímu importování.

 [Jak spravovat Kontrolu síťové komunikace v produktu ESET pro Windows](#) se dozvíte v článku z Databáze znalostí.

Zablokována síťová hrozba

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

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

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

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

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

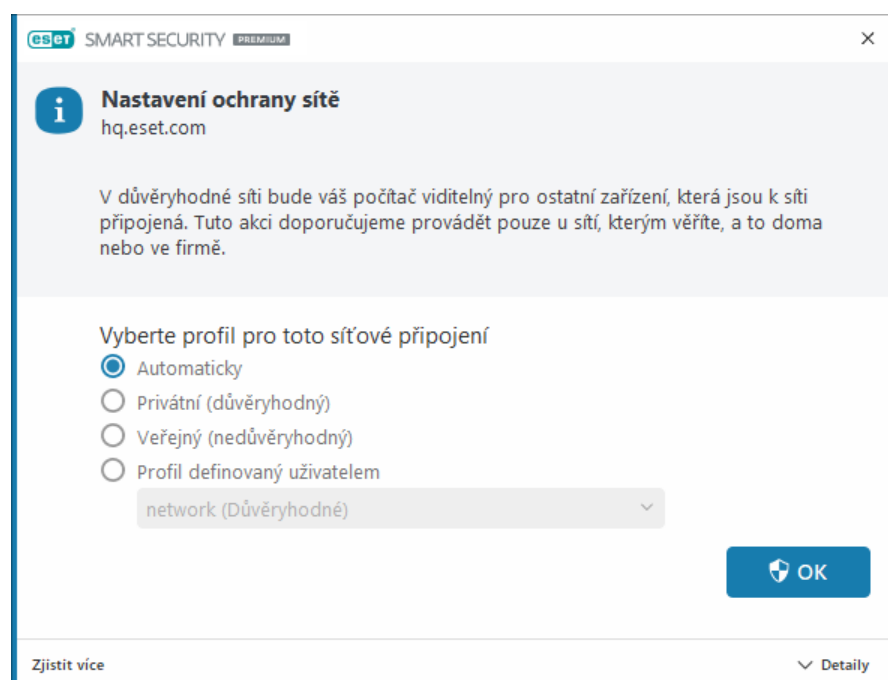
Zobrazená informace se může lišit podle detekované hrozby.

Pro více informací o hrozbách a souvisejících pojmech přejděte do kapitoly [Typy vzdálených útoků](#) nebo [i Typy detekcí](#).

Pro vyřešení situace, kdy dochází k zobrazování upozornění na **Duplicitní IP adresu v síti**, se podívejte do naší [Databáze znalostí](#).

Zjištěno připojení do nové sítě

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




Můžete si vybrat z následujících [profilů síťového připojení](#):

Automaticky – ESET Smart Security Premium vybere profil automaticky na základě [Spouštěčů](#) nakonfigurovaných pro každý profil.

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

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

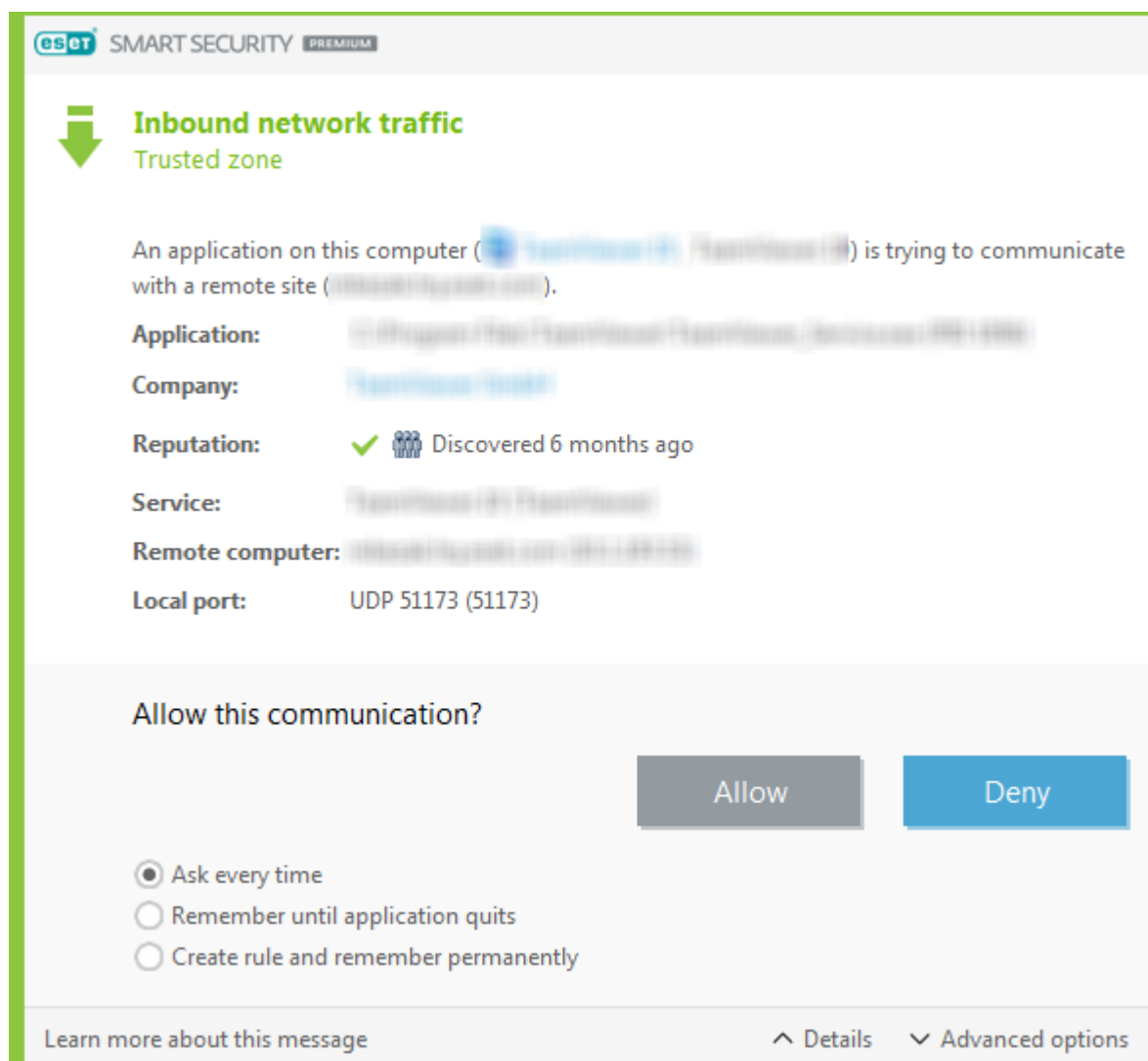
Profil definovaný uživatelem – z rozbalovacího menu můžete vybrat jeden z [profilů, které jste vytvořili](#). Tato možnost je k dispozici pouze v případě, že jste vytvořili alespoň jeden vlastní profil.

 Nesprávným nastavením sítě může být počítač ohrožen.

Navazování spojení – detekce

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

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



Při vytváření nových pravidel povolujte pouze spojení, která znáte a považujete je za bezpečná. Firewall při povolení všech spojení ztrácí svůj význam. Důležitými parametry spojení jsou zejména:

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

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

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

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

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

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

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

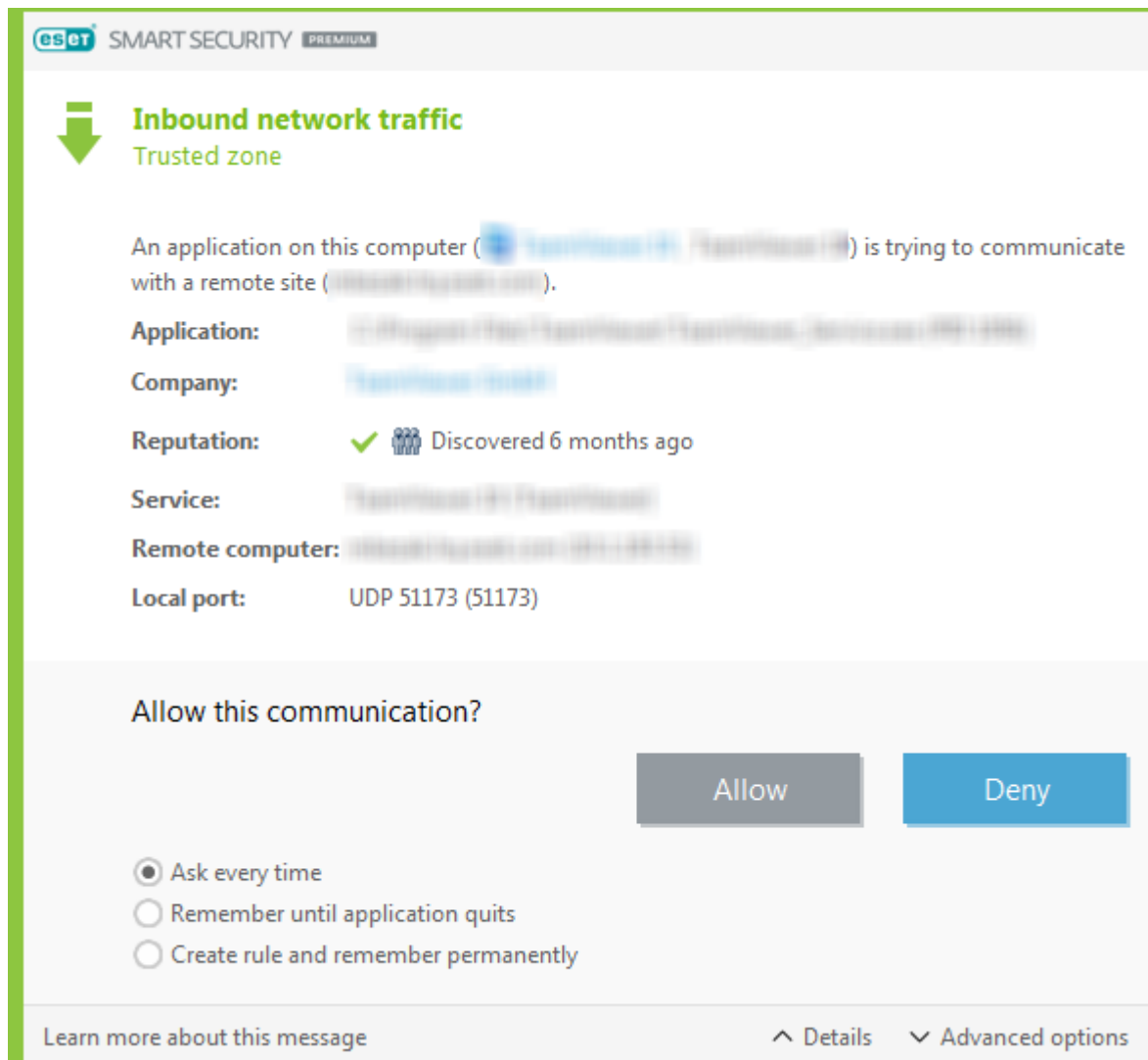
Změna aplikace

Firewall detekoval změnu aplikace, která již v minulosti navazovala komunikaci z počítače. Aplikace mohla být změněna například aktualizací na novější verzi. Ke změně aplikace mohlo také dojít infikováním nebezpečnou aplikací. Pokud si nejste jistí nutností změny v aplikaci, doporučujeme komunikaci aplikace zakázat a provést [Kontrolu počítače](#) s využitím [aktuálního detekčního jádra](#).

Příchozí důvěryhodná komunikace

Příklad příchozí komunikace uvnitř důvěryhodné zóny:

Vzdálený počítač z důvěryhodné zóny se pokouší navázat spojení s aplikací běžící ve vašem počítači.



Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

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

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

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

Lokální port – port použitý pro komunikaci.

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

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

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

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

Povolit – povolí příchozí komunikaci.


Zakázat – zakáže příchozí komunikaci.


Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí [editoru pravidel firewallu](#).

Odchozí důvěryhodná komunikace

Příklad odchozí komunikace z důvěryhodné zóny:


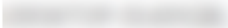
Aplikace běžící na lokálním počítači se snaží připojit na jiný počítač v lokální síti, nebo síti která byla označena jako důvěryhodná.

 SMART SECURITY PREMIUM





Odchozí síťová komunikace

Důvěryhodná zóna


Aplikace ( [Host Process for Windows Services](#), IP Helper) na tomto počítači se pokouší komunikovat se vzdáleným serverem 

Aplikace: C:\Windows\System32\svchost.exe (PID 852)

Společnost: [Microsoft Corporation](#)

Reputace:   Objeveno před rokem

Služba: IP Helper (iphlpvc)

Vzdálený počítač: 

Vzdálený port: UDP 59186 (59186)

Povolit tuto komunikaci?

Povolit

Zakázat

☐ Vždy se dotázat

☐ Zapamatovat akci do ukončení aplikace

☒ Vytvořit pravidlo a trvale zapamatovat

☒ Aplikace:

C:\Windows\System32\svchost.exe

☒ Služba:

iphlpvc

☒ Vzdálený počítač:

Důvěryhodná zóna

☐ Vzdálený port:

59186

☐ Lokální port:

63532

☒ Protokol:

TCP a UDP

☐ Upravit pravidlo před uložením

Zjistit více

^ Detaily ^ Další možnosti

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

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

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

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

Lokální port – port použitý pro komunikaci.

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

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

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

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí [editoru pravidel firewallu](#).

Příchozí komunikace

Příklad příchozí komunikace z internetu:

Vzdálený počítač se pokouší komunikovat s aplikací běžící na tomto počítači.

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

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

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

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

Lokální port – port použitý pro komunikaci.

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

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

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

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí [editoru pravidel firewallu](#).

Odchozí komunikace

Příklad odchozí komunikace z lokálního počítače do internetu:

Aplikace, která je spuštěna na lokálním počítači, se snaží připojit k internetu.

The screenshot shows the ESET Smart Security Premium interface for managing outgoing network communication. The title is "Odchozí síťová komunikace" (Outgoing network communication) with a sub-header "Internet".

The main section displays details for a specific communication attempt:

- Aplikace (Microsoft Edge Content Process)** na tomto počítači se pokouší komunikovat se vzdáleným serverem [redacted]
- Aplikace:** C:\Windows\SystemApps\Micr...\MicrosoftEdgeCP.exe (PID 3104)
- Společnost:** Microsoft Corporation
- Reputace:** [Green checkmark icon] [Group of people icon] Objeveno před 3 měsíci
- Vzdálený počítač:** [redacted]
- Vzdálený port:** TCP 443 (HTTPS)

Below this, a question "Povolit tuto komunikaci?" (Allow this communication?) is followed by two buttons: "Povolit" (Allow) and "Zakázat" (Deny).

Three radio buttons are available for future actions:

- ☐ Vždy se dotázat (Always ask)
- ☐ Zapamatovat akci do ukončení aplikace (Remember action until application ends)
- ☒ Vytvořit pravidlo a trvale zapamatovat (Create rule and remember permanently)

The bottom section allows for rule configuration with checkboxes and dropdown menus:

- ☒ **Aplikace:** C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe
- ☐ **Vzdálený počítač:** [redacted] (dropdown arrow)
- ☐ **Vzdálený port:** 443
- ☐ **Lokální port:** 1887
- ☒ **Protokol:** TCP a UDP (dropdown arrow)
- ☐ Upravit pravidlo před uložením (Edit rule before saving)

At the bottom, there is a link "Zjistit více" (Learn more) and two expandable sections: "Details" and "Další možnosti" (Other options).

Aplikace – aplikace, se kterou chce komunikovat vzdálené zařízení.

Cesta k aplikaci – umístění aplikace.

Aplikace z Microsoft Store – název aplikace v Microsoft Store.

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

Reputace – reputace aplikace získaná pomocí technologie ESET LiveGrid®.

Lokální port – port použitý pro komunikaci.

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

Lokální port – port použitý pro komunikaci.

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

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

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

Povolit – povolí příchozí komunikaci.

Zakázat – zakáže příchozí komunikaci.

Upravit pravidlo – umožňuje upravit vlastnosti pravidla pomocí [editoru pravidel firewallu](#).

Možnosti zobrazení spojení

Kliknutím pravým tlačítkem na spojení se zobrazí následující možnosti:

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

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

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

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

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

Aktualizovat nyní – kliknutím aktualizujete obsah okna **Síťová spojení**.

Bezpečnostní nástroje

Otevřete [hlavní okno programu](#) > **Nastavení** > **Bezpečnostní nástroje** a nastavte následující moduly:

Zabezpečené bankovníctví a prohlížení webu – přidává do prohlížeče další ochrannou vrstvu, která chrání vaše finanční údaje během online transakcí. Zapněte **Zabezpečení všech prohlížečů** v [rozšířeném nastavení Zabezpečeného bankovníctví a prohlížení webu](#), aby se všechny [podporované webové prohlížeče](#) spouštěly v zabezpečeném režimu.

Ochrana soukromí a zabezpečení v prohlížeči – zajišťuje soukromí a bezpečnost vašich online aktivit, aniž byste zanechávali digitální stopu.

Anti-Theft – [Anti-Theft](#) chrání vaše zařízení v případě ztráty nebo krádeže.

Secure Data – po zapnutí [Secure Data](#) můžete šifrovat svá data a zabránit zneužití citlivých a důvěrných informací.

Password Manager – [Password Manager](#) chrání a ukládá vaše hesla a osobní údaje.


Zabezpečené bankovníctví a prohlížení webu

Zabezpečené bankovníctví a prohlížení webu představuje další vrstvu ochrany, která má chránit vaše finanční údaje během online transakcí.

Ve výchozím nastavení se budou všechny podporované prohlížeče spouštět v zabezpečeném režimu. Díky tomu můžete prohlížet webové stránky, používat internetové bankovníctví a provádět online transakce v jednom zabezpečeném prohlížeči.



Reputační systém ESET LiveGrid® musí být zapnutý (ve výchozím nastavení je zapnutý), aby bylo zajištěno správné fungování Zabezpečeného bankovníctví a prohlížení webu.

Jak konfigurovat zabezpečený prohlížeč se dozvíte v kapitole [Rozšířená nastavení Zabezpečeného bankovníctví a prohlížení webu](#). Pokud vypnete funkci **Zabezpečit všechny prohlížeče**, můžete se k zabezpečenému prohlížeči dostat z [hlavního okna programu](#) > **Přehled** > **Zabezpečené bankovníctví a prohlížení webu** nebo z pracovní plochy pomocí zástupce  **Zabezpečené bankovníctví a prohlížení webu**. V takovém případě se v zabezpečeném režimu spustí internetový prohlížeč, který máte ve Windows nastaven jako výchozí.

Pro zajištění zabezpečeného prohlížení internetu je nezbytné použití HTTPS šifrované komunikace. Následující prohlížeče podporují Zabezpečené bankovníctví a prohlížení webu:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+



Na zařízeních s procesory ARM je tato funkce podporována pouze v prohlížeči Firefox a Microsoft Edge.

Další podrobnosti o funkcích Zabezpečeného bankovníctví a prohlížení webu naleznete v následujících článcích v

Databázi znalostí ESET:

- [Jak používat Zabezpečené bankovníctví a prohlížení webu?](#)
- [Pozastavení nebo vypnutí Zabezpečeného bankovníctví a prohlížení webu v produktech ESET určených pro domácnosti používající systém Windows](#)
- [ESET Zabezpečené bankovníctví a prohlížení webu – nejčastější chyby](#)
- [Slovník pojmů ESET | Zabezpečené bankovníctví a prohlížení webu](#)


Oznámení v prohlížeči

Zabezpečený prohlížeč vás o své stavu informuje prostřednictvím oznámení zobrazovaných v prohlížeči a barevným rámečkem kolem jeho okna.

Oznámení v prohlížeči se zobrazuje v záložce na pravé straně okna prohlížeče.



Oznámení v prohlížeči si rozbalíte kliknutím na ikonu ESET . Kliknutím na oznámení jej minimalizujete. Chcete-li oznámení a zelený rámeček prohlížeče skrýt, klikněte na ikonu  (zavřít).

 Zrušit lze pouze informativní oznámení a zelený rámeček prohlížeče.

Oznámení v prohlížeči

Typ oznámení	Stav
Informativní oznámení a zelený rámeček prohlížeče	Je zajištěna maximální ochrana a oznámení v prohlížeči je ve výchozím nastavení minimalizované. Rozbalte oznámení v prohlížeči a po kliknutí na Nastavení otevřete Bezpečnostní nástroje .
Upozornění a oranžový rámeček prohlížeče	Zabezpečený prohlížeč vyžaduje vaši pozornost pro nekritické problémy. Pro zobrazení souvisejících informací nebo řešení postupujte podle kroků uvedených v oznámení v prohlížeči.
Bezpečnostní upozornění a červený rámeček prohlížeče	Prohlížeč není chráněn modulem ESET Zabezpečené bankovníctví a prohlížení webu. Pro zajištění ochrany restartujte prohlížeč. Pro kontrolu konfliktů se soubory načtenými v prohlížeči si otevřete Protokoly > Zabezpečené bankovníctví a prohlížení webu a zajistěte, aby při dalším spuštění prohlížeče nebyly zaznamenané soubory načtené. Pokud problémy přetrvávají, pro vyřešení konfliktu se soubory načtenými prohlížečem kontaktujte technickou podporu společnosti ESET podle pokynů uvedených v naší Databázi znalostí .

Ochrana soukromí a zabezpečení v prohlížeči

Ochranu soukromí a zabezpečení v prohlížeči můžete zapnout jako rozšíření dostupné v podporovaných prohlížečích (pouze [Google Chrome](#), [Mozilla Firefox](#) a [Microsoft Edge](#)).


Instalace a povolení rozšíření:

1. Ujistěte se, že používáte nejnovější verzi ESET Smart Security Premium, a po případné aktualizaci restartujte počítač.
2. Otevřete prohlížeč.
3. Rozšíření je nainstalováno v prohlížeči.
4. Povolte rozšíření a v prohlížeči se zobrazí stránka s podrobnostmi o rozšíření.

Hlavní nabídka rozšíření Ochrana soukromí a zabezpečení v prohlížeči je rozdělena do následujících sekcí:


Přehled

Zabezpečené vyhledávání

Pomocí přepínače  vedle položky **Kontrolovat výsledky vyhledávání** tuto funkci zapnete a uvidíte, na které výsledky lze bezpečně kliknout. Zabezpečené vyhledávání vyhodnocuje adresy odkazů v seznamu, což nemusí nutně znamenat, že webová stránka neobsahuje škodlivý kód. Naše detekční jádro pak na této webové stránce odhalí škodlivý kód.

Vyčištění prohlížeče


Vymažte data o prohlížení internetu nebo nastavte jejich pravidelné čištění. Webové stránky, u kterých chcete přijímat cookies a zůstat přihlášení i po vyčištění prohlížeče, můžete přidat do **seznamu**.

- **Jednorázové čištění** – z rozbalovacího menu vyberte časový rozsah a typ dat, která chcete odstranit. Můžete zvolit všechna data, soukromá data nebo data podle vlastního výběru.
- **Pravidelné čištění** – kliknutím na přepínač  vedle položky **Pravidelné čištění** povolíte tuto funkci. Z rozbalovacího menu vyberte časový rozsah a typ dat, která chcete pravidelně odstraňovat. Můžete zvolit všechna data, soukromá data nebo data podle vlastního výběru.


Vlastní data mají následující kategorie:

- Historie prohlížení internetu
- Historie stahování
- Cookies a údaje o webových stránkách
- Obrázky a soubory v mezipaměti
- Hesla a přihlašovací údaje
- Data automatického vyplňování formulářů

Vyčištění metadat

Funkce Vyčištění metadat kontroluje soukromá data odhalitelná prostřednictvím metadat ve formátu EXIF sdílených v mediálních souborech, dokumentech a dalších podporovaných formátech souborů. Kliknutím na přepínač  vedle položky **Vyčistit metadata při každém nahrání obrázku** zapnete odstraňování metadat.

 Je nutné restartovat prohlížeč, **Vyčištění metadat** fungovalo správně.

Kliknutím na přepínač  vedle položky **Dostávat oznámení v prohlížeči** povolíte zobrazování oznámení po Vyčištění metadat.

Přehled nastavení webových stránek


Přístup k nastavení oprávnění webových stránek umožňuje kontrolovat, jaké informace mohou webové stránky používat.


- **Oznámení** – webové stránky, u kterých chcete **povolit/blokovat** oznámení nebo zda chcete, aby se vás rozšíření prohlížeče **pokaždé zeptalo**.

Rozšířená nastavení

Vyčištění prohlížeče

Pokročilé nastavení cookies

Přidejte do seznamu webové stránky, na kterých chcete přijímat cookies a zůstat přihlášení i po vyčištění prohlížeče. Do textového pole zadejte URL adresu a klikněte na **Přidat**. Ze seznamu ji můžete kdykoli odstranit kliknutím na ikonu minus  vedle konkrétní webové stránky.

V dolní části stránky je seznam navrhovaných domén, které jsou aktuálně otevřeny v prohlížeči. Pokud určitou webovou stránku nevidíte, klikněte na **obnovit seznam** a přidejte ji do seznamu přijatých cookies kliknutím na ikonu plus .

Přehled nastavení webových stránek

Přístup k nastavení oprávnění webových stránek umožňuje kontrolovat, jaké informace mohou webové stránky používat.

- **Oznámení** – webové stránky, u kterých chcete **povolit/blokovat** oznámení nebo zda chcete, aby se vás rozšíření prohlížeče **pokaždé zeptalo**.

Vzhled

Přizpůsobte si barevné schéma rozhraní podle svých preferencí. Zaškrtnutím políčka **Světlý** nebo **Tmavý** můžete zvolit preferovaný barevný režim.

Anti-Theft

Osobní zařízení jsou neustále vystavena riziku ztráty nebo krádeže během našich každodenních cest z domova do práce nebo na jiná veřejná místa. Anti-Theft je funkce, která rozšiřuje zabezpečení uživatele v případě ztráty nebo krádeže zařízení. Anti-Theft umožňuje sledovat používání zařízení a dohledat ztracené zařízení pomocí lokalizace podle IP adresy ve [ESET HOME](#), čímž vám pomůže získat zařízení zpět a ochránit osobní údaje.

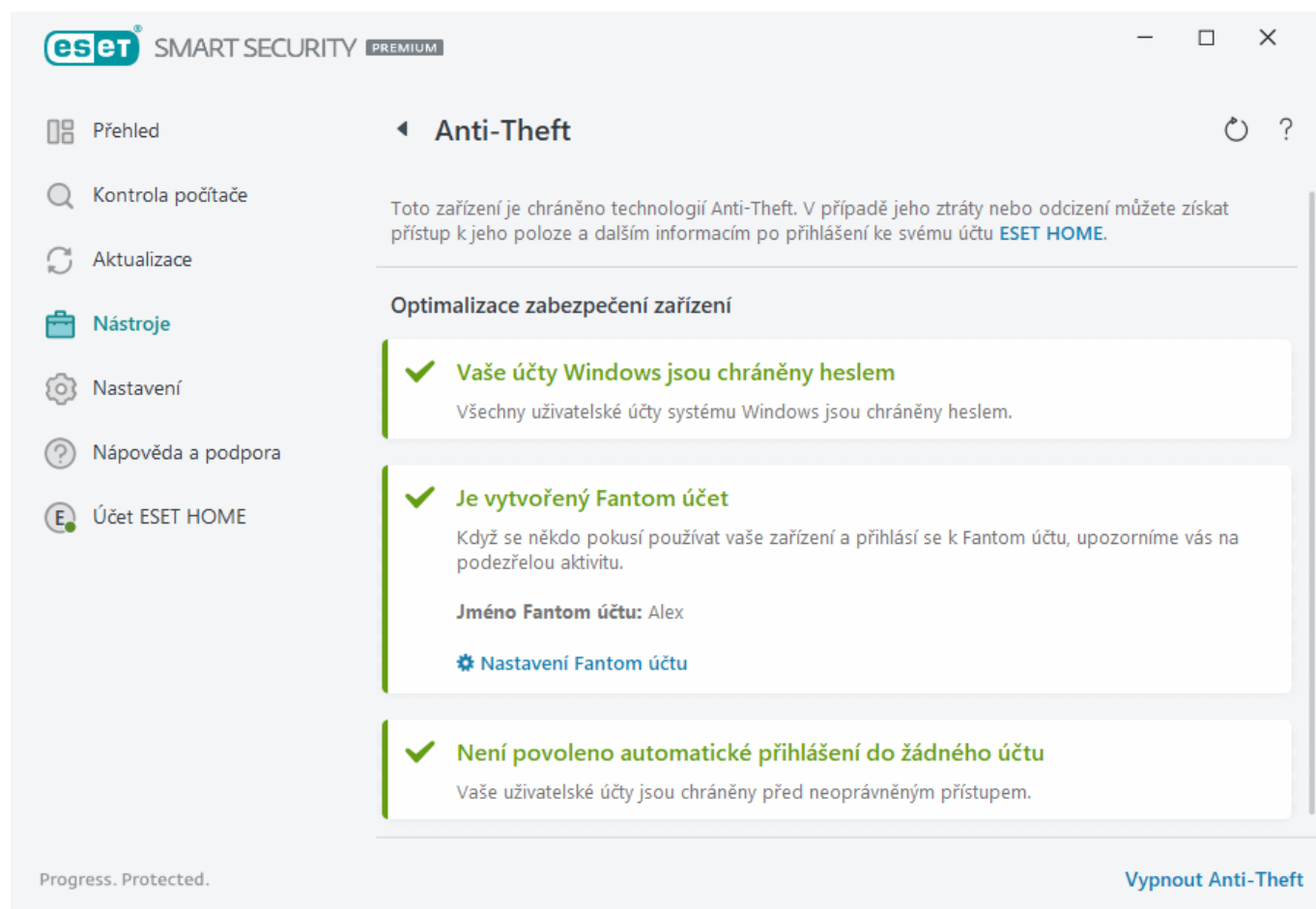
Pomocí moderních technologií, jako je vyhledávání zařízení podle IP adresy, vzdálená aktivace webové kamery nebo uzamknutí uživatelských účtů, Anti-Theft ochrání data uložená ve vašem počítači či jiném zařízení v případě jeho ztráty nebo odcizení a zároveň vám pomůže zjistit jeho polohu. Stejně tak následně na [ESET HOME](#) můžete

sledovat aktivity na vašem počítači nebo mobilním zařízení pohodlně prostřednictvím internetového prohlížeče nebo mobilní aplikace.

Více informací týkající se technologie Anti-Theft naleznete v [online příručce k portálu ESET HOME](#).

! Anti-Theft nemusí správně fungovat u počítačů připojených do domény kvůli omezením ve správě uživatelských účtů.

Po [zapnutí funkce Anti-Theft](#) si nastavte způsob zabezpečení svého zařízení v [hlavním okně programu](#) > **Nastavení** > **Bezpečnostní nástroje** > **Anti-Theft**.



Možnosti optimalizace

Není vytvořen žádný Fantom účet

Vytvořte si Fantom účet, abyste zvýšili šanci na nalezení ztraceného nebo odcizeného zařízení. Pokud zařízení označíte jako ztracené, Anti-Theft zablokuje přístup k aktivním uživatelským účtům, a tím ochrání vaše osobní data uložená v zařízení. Každý, kdo se pokusí zařízení používat, bude moci použít pouze Fantom účet. Fantom účet je forma účtu hosta, který má omezené oprávnění. Dokud zařízení neoznačíte jako nalezené, bude tento účet používán jako výchozí – tím bude zabráněno komukoli v přihlášení k jiným uživatelským účtům nebo v přístupu k datům uživatele.

i Jestliže se někdo přihlásí k Fantom účtu, pokud je váš počítač v normálním stavu, zašleme vám e-mailem oznámení s informacemi o podezřelé aktivitě na počítači. Po obdržení e-mailového oznámení se můžete rozhodnout, zda chcete počítač označit jako ztracený.

Pro vytvoření Fantom účtu klikněte na možnost **Vytvořit Fantom účet**, do textového pole zadejte **název Fantom účtu** a klikněte na tlačítko **Vytvořit**.

Pokud již Fantom účet máte vytvořen, kliknutím na možnost **Nastavení Fantom účtu** jej můžete přejmenovat nebo odstranit.

Zabezpečení účtů Windows heslem

Váš uživatelský účet není chráněn heslem Toto upozornění na optimalizaci se zobrazí, pokud alespoň jeden uživatelský účet není chráněn heslem. Problém v počítači vyřešíte nastavením hesla všem uživatelům (s výjimkou **Fantom účtu**).

Pro nastavení hesla k uživatelskému účtu klikněte na možnost **Spravovat Windows účty** nebo postupujte podle následujících pokynů:

1. Stiskněte klávesy CTRL+Alt+Delete.
2. Klikněte na **Změnit heslo**.
3. Pole **Původní heslo** ponechte prázdné.
4. Heslo zadejte dvakrát do polí **Nové heslo** a **Potvrzení hesla**.

Automatické přihlášení k účtu Windows


Do svého uživatelského účtu máte nastaveno automatické přihlášení, a není chráněn před neoprávněným přístupem. Toto upozornění na optimalizaci se zobrazí, pokud alespoň do jednoho uživatelského účtu je povoleno automatické přihlášení. Kliknutím na **Vypnout automatické přihlášení** vyřešíte tento problém s optimalizací.

Automatické přihlášení k Fantom účtu

Na vašem zařízení je povoleno automatické přihlášení k **Fantom účtu**. Pokud je zařízení v normálním stavu, nedoporučujeme používat automatické přihlášení, protože to může způsobit problémy s přístupem k vašemu skutečnému uživatelskému účtu, resp. může docházet ke generování falešných poplachů související se ztrátou/odcizením vašeho počítače. Kliknutím na **Vypnout automatické přihlášení** vyřešíte tento problém s optimalizací.

Přihlášení k účtu ESET HOME


Pokud chcete zapnout/vypnout Anti-Theft a získat přístup k poloze a informacím o zařízení v portálu [ESET HOME](#), přihlaste se ke svému ESET HOME účtu.


 SMART SECURITY PREMIUM


ESET HOME | Anti-Theft


V případě ztráty nebo odcizení zařízení využijte účet ESET HOME k získání nejen polohy zařízení, ale i dalších informací.

Přihlášení k účtu ESET HOME

 Přihlásit se pomocí Google

 Přihlásit se pomocí Apple


 Naskenovat QR kód

 HOME

E-mailová adresa

Heslo

[Zapomněli jste heslo?](#)

 Přihlásit se


Zrušit

Nemáte účet? [Vytvořte si jej!](#)

K účtu ESET HOME se přihlásíte pomocí jednoho z uvedených způsobů:

- **Pomocí e-mailové adresy a hesla k účtu ESET HOME** – Zadejte svou **e-mailovou adresu** a **heslo**, které jste použili při vytvoření účtu ESET HOME, a klikněte na tlačítko **Přihlásit se**.
- **Pomocí svého účtu Google/AppleID** – Klikněte na tlačítko **přihlášení prostřednictvím Google**, případně **Apple** a přihlaste se příslušným účtem. Po úspěšném přihlášení vás přesměrujeme na potvrzovací webovou stránku portálu ESET HOME. Pro pokračování klikněte zpět do produktu ESET. Další informace o přihlášení pomocí účtů Google/AppleID naleznete v [Online nápovědě k ESET HOME](#).
- **Naskenovat QR kód** – Kliknutím na příslušné tlačítko **zobrazíte QR kód** pro přihlášení. Otevřete si mobilní aplikaci ESET HOME a naskenujte QR kód, případně QR kód zaměřte fotoaparátem zařízení. Další informace naleznete v [Online nápovědě k ESET HOME](#).

Neúspěšné přihlášení – běžné chyby.

 Pokud zatím nemáte účet ESET HOME, pro registraci nebo zobrazení instrukcí v [Online nápovědě ESET HOME](#) klikněte na tlačítko **Vytvořit účet**.
V případě, že si na heslo nemůžete vzpomenout, klikněte na možnost **Zapomněli jste heslo?** a pokračujte dle instrukcí v [Online nápovědě ESET HOME](#).

 Anti-Theft nepodporuje Microsoft Windows Home Server.

Zadejte název zařízení

V poli **Název počítače** najdete jméno, které bude sloužit jako identifikátor zařízení na portálu [ESET HOME](#). Název počítače je standardně automaticky předvyplněný. Zadejte název zařízení nebo použijte výchozí název a klikněte na **Dokončit** (Pokračovat).

Anti-Theft je zapnutý/vypnutý

Toto okno obsahuje potvrzovací zprávu, pokud zapnete nebo vypnete Anti-Theft:

- Zapnuto – Zařízení je chráněno technologií Anti-Theft. Funkci a jí chráněná zařízení spravujte vzdáleně ve stejnojmenné části [portálu ESET HOME](#) prostřednictvím svého účtu.
- Vypnuto – Anti-Theft je na tomto zařízení vypnutý a všechna data související s funkcí <%ESET_ANTTHEFT%> na tomto zařízení jsou z portálu ESET HOME odebrána.

Přidání nového zařízení selhalo

Při aktivaci Anti-Theft jste obdrželi chybové hlášení.

Nejčastější problémy s aktivací mohou být:


- [Chyba při přihlašování k účtu ESET HOME](#)
- Zařízení není připojeno k internetu (nebo připojení právě nefunguje).

V případě přetrvávajících potíží kontaktujte [technickou podporu společnosti ESET](#).

Secure Data

Secure Data je funkce v ESET Smart Security Premium, která umožňuje šifrovat data na vašem počítači a chránit výměnná média před zneužitím soukromých či tajných informací. Nejčastější dotazy týkající se součástí Secure Data naleznete v [ESET Databázi znalostí](#) (článek nemusí být dostupný ve všech jazycích).

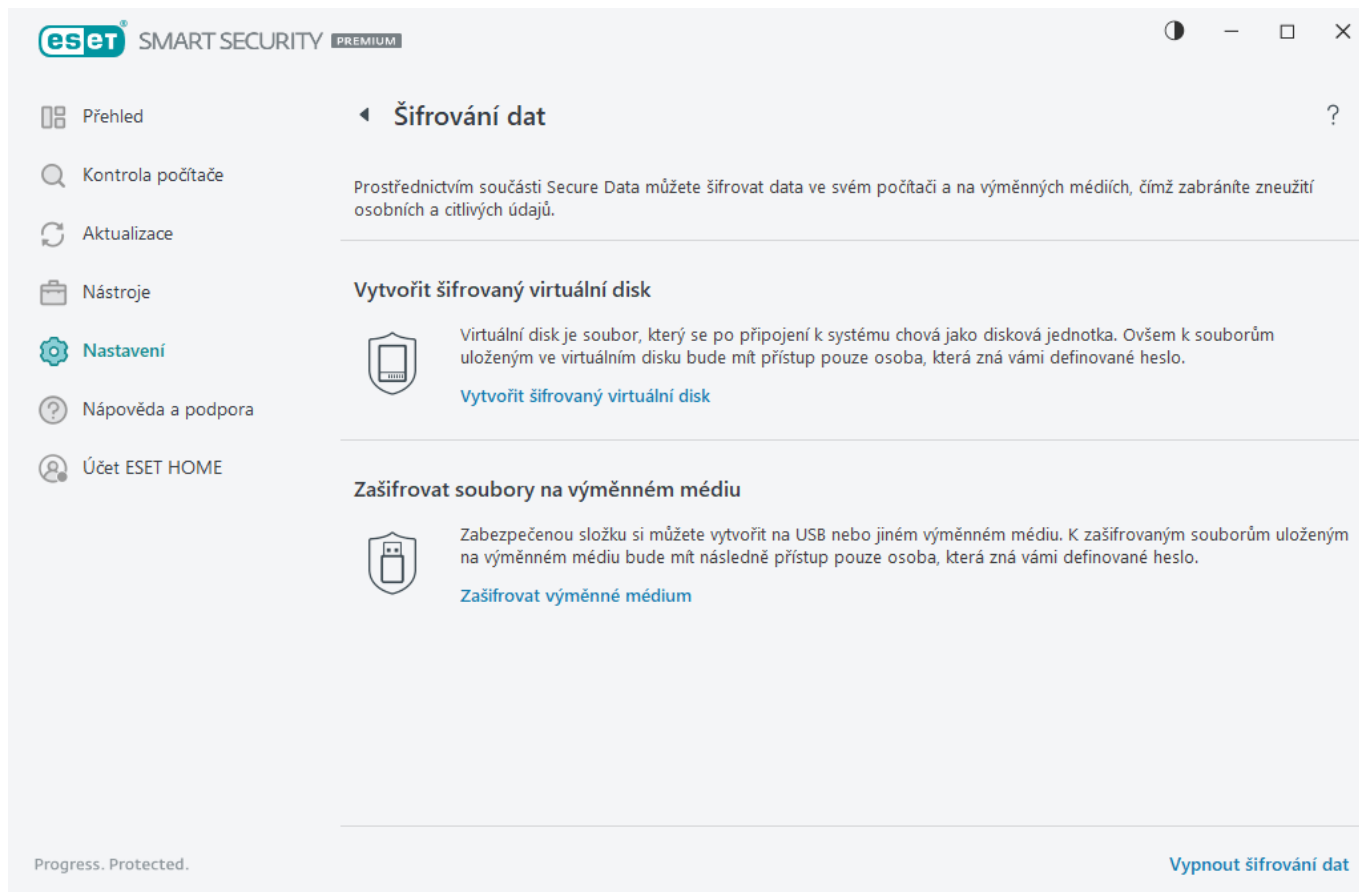
Pro zapnutí Secure Data zvolte jednu z následujících možností:

- V [hlavním okně programu](#) v části **Přehled** klikněte na **NASTAVIT** vedle položky **Secure Data**.
- V [hlavním okně programu](#) v části **Nastavení > Bezpečnostní nástroje** přepínačem aktivujte  **Secure Data**.

i Na zařízení, na kterém máte zapnuté Secure Data, není možné dále nainstalovat ESET Endpoint Encryption.

Pokud máte Secure Data zapnuté, v [hlavním okně programu](#) klikněte na **Nastavení > Bezpečnostní nástroje > Secure Data** a vyberte jednu z následujících možností:

- [Vytvoření šifrovaného virtuálního disku](#)
- [Zašifrovat soubory na výměnném médiu](#)



Vytvořit šifrovaný virtuální disk

Prostřednictvím Secure Data si můžete vytvořit libovolné množství šifrovaných virtuálních disků. Limitováni jste pouze volným místem na disku. Pro vytvoření virtuálního šifrovaného disku postupujte podle následujících kroků:

1. V [hlavním okně programu](#) přejděte na záložku **Nastavení** > **Bezpečnostní nástroje** > **Secure Data** > **Vytvořit šifrovaný virtuální disk**.
2. V dalším kroku klikněte na tlačítko **Procházet** a vyberte místo, kam chcete virtuální disk uložit.
3. Zadejte název virtuálního disku a klikněte na možnost **Uložit**.
4. Z rozbalovacího menu **Maximální kapacita** vyberte velikost virtuálního disku a klikněte na tlačítko **Pokračovat**.
5. V dalším kroku si nastavte heslo, kterým chcete chránit přístup k šifrovanému virtuálnímu disku. Pokud nechcete automaticky virtuální disk dešifrovat po přihlášení ke svému Windows účtu, odškrtněte možnost **Automaticky dešifrovat na tomto Windows účtu**. Klikněte na tlačítko **Pokračovat**.
6. Klikněte na **Hotovo**. Váš šifrovaný virtuální disk je vytvořen a připraven k použití. Zobrazí se jako lokální disk v části **Tento počítač**.

Pro přístup do šifrovaného disku po restartu počítače vyhledejte vámi vytvořený soubor (.eed) a poklepejte na něj dvojklikem. Pokud budete požádáni, zadejte heslo, které jste nastavili během vytváření šifrovaného disku. Jednotka bude připojena a zobrazí se jako lokální disk v části Tento počítač. Jakmile se šifrovaný disk připojí jako lokální, bude jeho dešifrovaný obsah přístupný všem ostatním uživatelům počítače, dokud se neodhlásíte nebo nerestartujete počítač.

Mohu virtuální disk smazat?

- i** Ano. Pro smazání šifrovaného virtuálního disku postupujte dle instrukcí uvedených v [ESET Databázi znalostí](#) (článek nemusí být dostupný ve všech jazycích).

Zašifrovat soubory na výměnném médiu

Prostřednictvím součásti Secure Data můžete na výměnných médiích vytvořit šifrované složky. Pro zašifrování souborů na výměnném médiu:

1. Připojte k počítači výměnné médium (USB flash disk, externí HDD).
2. V [hlavním okně programu](#) přejděte na záložku **Nastavení > Bezpečnostní nástroje > Secure Data > Zašifrovat soubory na výměnném médiu**.
3. Z rozbalovacího menu vyberte výměnné médium a klikněte na tlačítko **Pokračovat**.
Pro obnovení seznamu dostupných zařízení klikněte na tlačítko **Aktualizovat**. Šifrovaná a nepodporovaná média nebudou zobrazena.
Pokud chcete mít přístup šifrovaným složkám i na zařízeních, na kterých není nainstalován ESET Smart Security Premium, vyberte možnost **Dešifrovat složku na jakémkoli Windows zařízení**.
4. V dalším kroku si nastavte heslo, kterým chcete chránit přístup k šifrovanému disku. Pokud nechcete automaticky virtuální disk dešifrovat po přihlášení ke svému Windows účtu, odškrtněte možnost **Automaticky dešifrovat na tomto Windows účtu**. Klikněte na tlačítko **Pokračovat**.
5. Vaše výměnné médium je chráněno a šifrované adresáře jsou připraveny k použití.

Pokud výměnné médium připojíte k počítači, na kterém není Secure Data zapnuté, šifrovaná složka nebude viditelná. Pokud připojíte disk k počítači se zapnutým Secure Data, budete vyzváni k zadání hesla pro dešifrování výměnného média. Ne zadáte-li heslo, šifrovanou složku uvidíte, ale nebude přístupná.

Password Manager

Password Manager je součástí balíčku ESET Smart Security Premium.

Jedná se o správce hesel, který si pamatuje hesla za vás a automaticky je doplňuje na webových stránkách a v aplikacích. Přihlašovací údaje ukládá do bezpečného a šifrovaného úložiště, které je chráněno hlavním heslem – to jediné si musíte pamatovat.

Další informace naleznete v [online příručce k Password Manager](#):

- [Instalace Password Manager](#)
- [Registrace Password Manager](#)
- [Správa úložišť Password Manager na portálu ESET HOME](#)

Import a export nastavení

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

Názorné ukázky

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

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

Pro importování nastavení přejděte v [hlavním okně programu](#) na záložku **Nastavení**, klikněte na tlačítko **Import a export nastavení** a v zobrazeném dialogovém okně vyberte možnost **Import nastavení**. Zadejte cestu k souboru s konfigurací, případně klikněte na ... a najděte soubor, který chcete importovat.

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

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

The screenshot shows the 'Import a export nastavení' dialog box in the ESET Smart Security Premium interface. At the top, there is a title bar with the ESET logo and 'SMART SECURITY PREMIUM' on the left, and a close button (X) on the right. Below the title bar, the dialog has a header 'Import a export nastavení' with a help icon (?). The main text area contains the instruction: 'Aktuální konfiguraci produktu si můžete uložit do XML souboru a později nebo na jiném počítači ji z tohoto souboru obnovit.' Below this, there are two radio buttons: 'Import nastavení' (which is selected) and 'Export nastavení'. Underneath the radio buttons is a text field labeled 'Cesta k souboru:' followed by a button with three dots (...). At the bottom of the dialog, there are two buttons: 'Importovat' (with a shield icon) and 'Zavřít'.

Nápověda a podpora

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



Předplatné

- [Průvodce řešením problémů s předplatným](#) – po kliknutí si zobrazíte nejčastější problémy týkající se aktivace nebo změny předplatného společně s jejich řešením.
- [Změnit předplatné](#) – po kliknutí se zobrazí dialogové okno, pomocí kterého můžete produkt aktivovat. Pokud je vaše zařízení [připojeno k ESET HOME](#), vyberte předplatné z účtu ESET HOME nebo přidejte nové.



Nainstalovaný produkt

- [Co je nového](#) – po kliknutí na odkaz se otevře okno s informacemi o nových a vylepšených funkcích.
- [O programu ESET Smart Security Premium](#) – kliknutím si zobrazíte souhrnné informace o vámi nainstalovaném programu ESET Smart Security Premium.
- [Průvodce řešením problémů s produktem](#) – kliknutím na tento odkaz naleznete řešení nejčastějších problémů.
- **Změnit produkt** – kliknutím zjistíte, zda lze ESET Smart Security Premium změnit na [jinou produktovou řadu](#) s aktuálním předplatným.



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



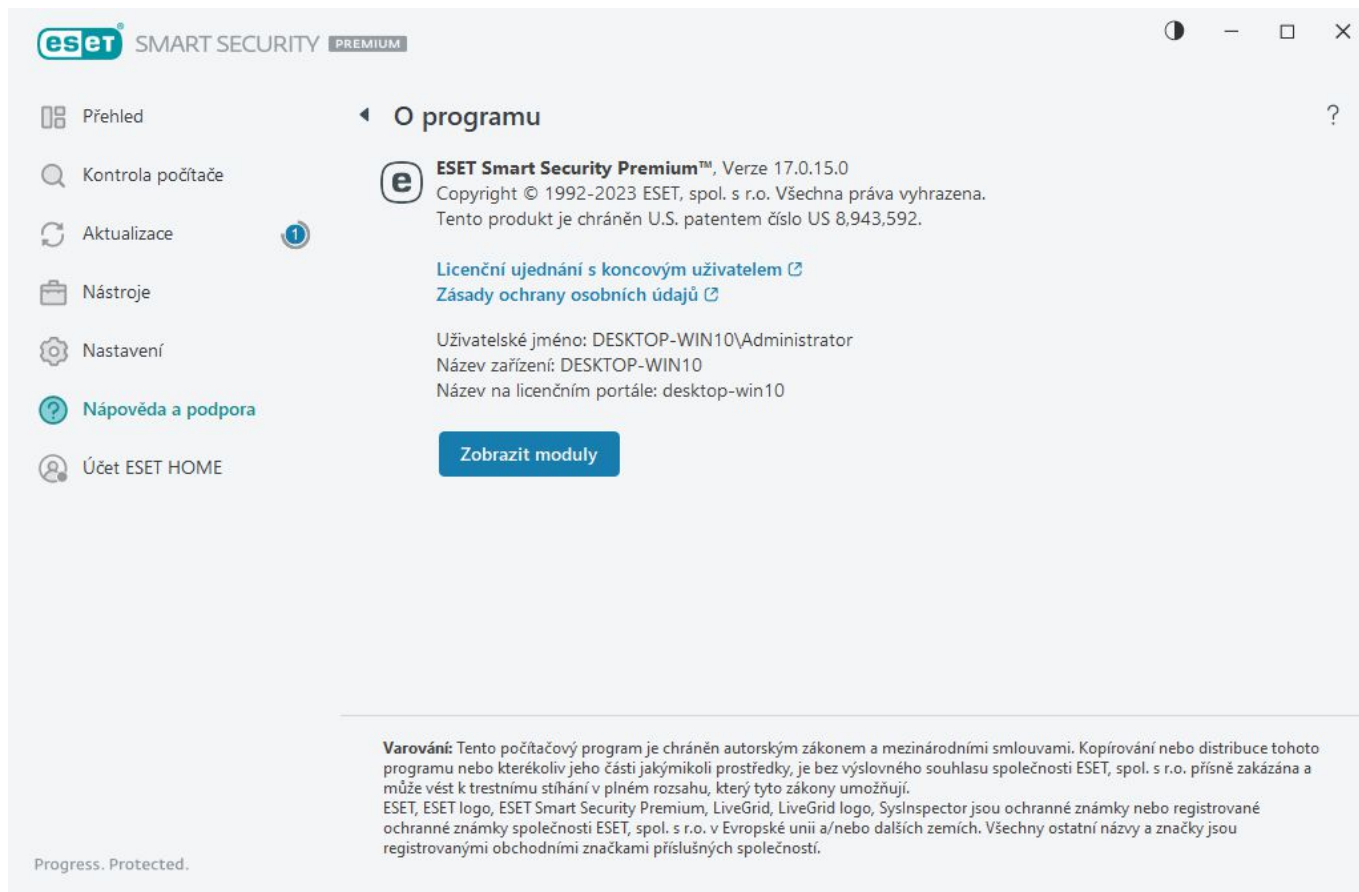
[Technická podpora](#)



Databáze znalostí – internetová [ESET Databáze znalostí](#) obsahuje odpovědi na často kladené otázky a doporučené způsoby pro řešení problémů. Databáze znalostí, pravidelně aktualizovaná technickými specialisty společnosti ESET, je nejmocnějším nástrojem při řešení nejrůznějších problémů.

O programu ESET Smart Security Premium

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



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

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

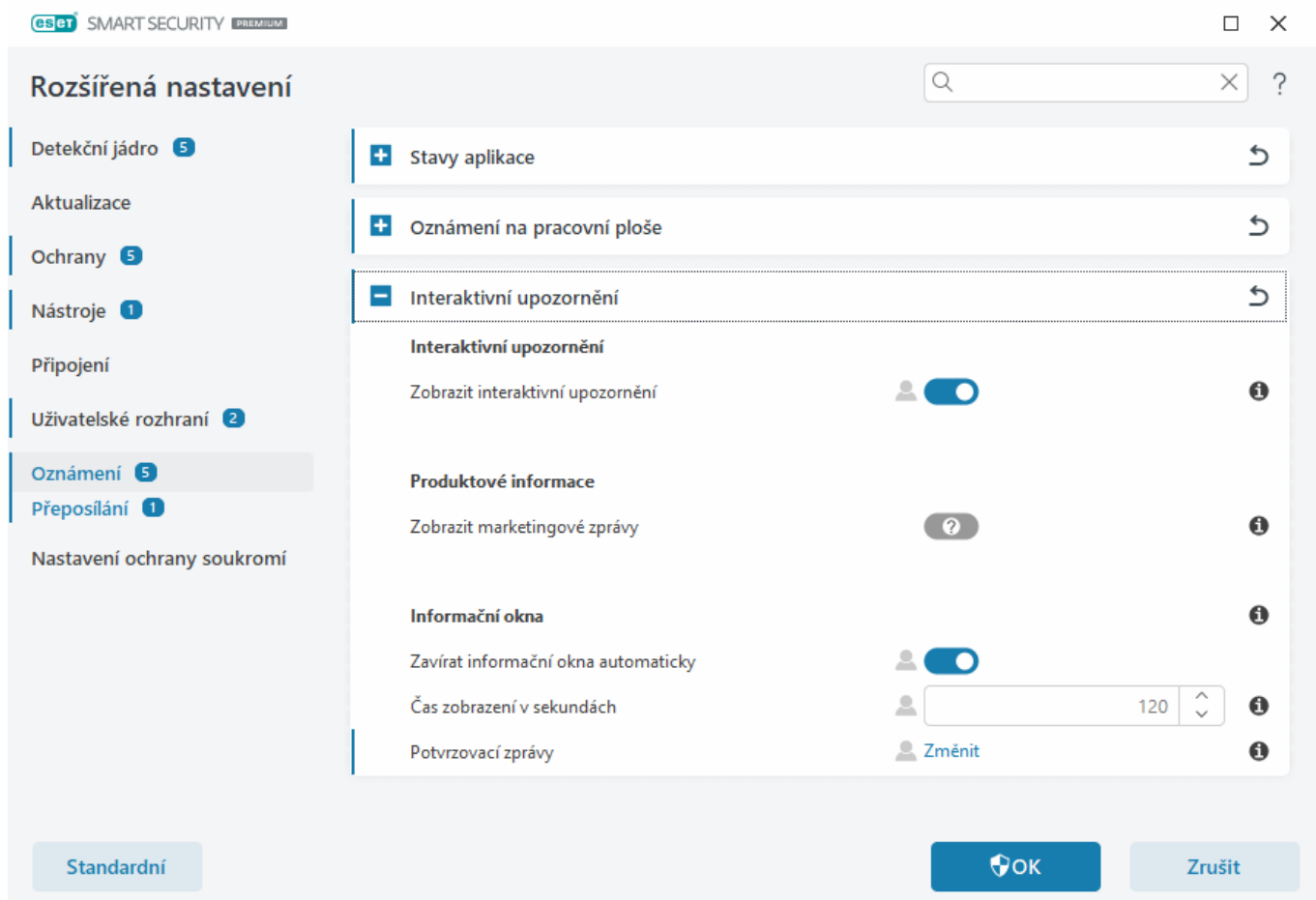
ESET Novinky

V této části ESET Smart Security Premium vás budeme informovat o novinkách a výhodných akcích produktů ESET.

Zobrazení marketingových zpráv (tzv. in-product messaging) bylo navrženo pro informování uživatelů o novinkách a akcích společnosti ESET. Příjem marketingových zpráv vyžaduje váš souhlas. Ve výchozím stavu je u této položky zobrazena ikona otazníku a žádné zprávy nejsou zasílány. Zapnutím možnosti souhlasíte s jejich zasíláním. Pokud o sdělení nemáte zájem, pomocí přepínače na řádku **Zobrazit marketingové zprávy** možnost vypněte.

Chcete-li povolit nebo zakázat příjem marketingových zpráv prostřednictvím oznamovacího okna, postupujte dle následujících instrukcí.

1. Otevře [Rozšířená nastavení](#).
2. Dále přejděte do sekce **Oznámení > Interaktivní upozornění**.
3. Upravte pomocí přepínače možnost **Zobrazit marketingové zprávy**.



Odeslat konfiguraci systému

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

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

Odesílání údajů o konfiguraci systému můžete nastavit v [Rozšířených nastaveních](#) > **Nástroje** > **Diagnostika** > [Technická podpora](#).



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

Technická podpora

V [hlavním okně programu](#) přejděte na záložku **Nápověda a podpora**, klikněte na **Technická podpora**.

Kontaktovat Technickou podporu

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

Získání informací pro technickou podporu

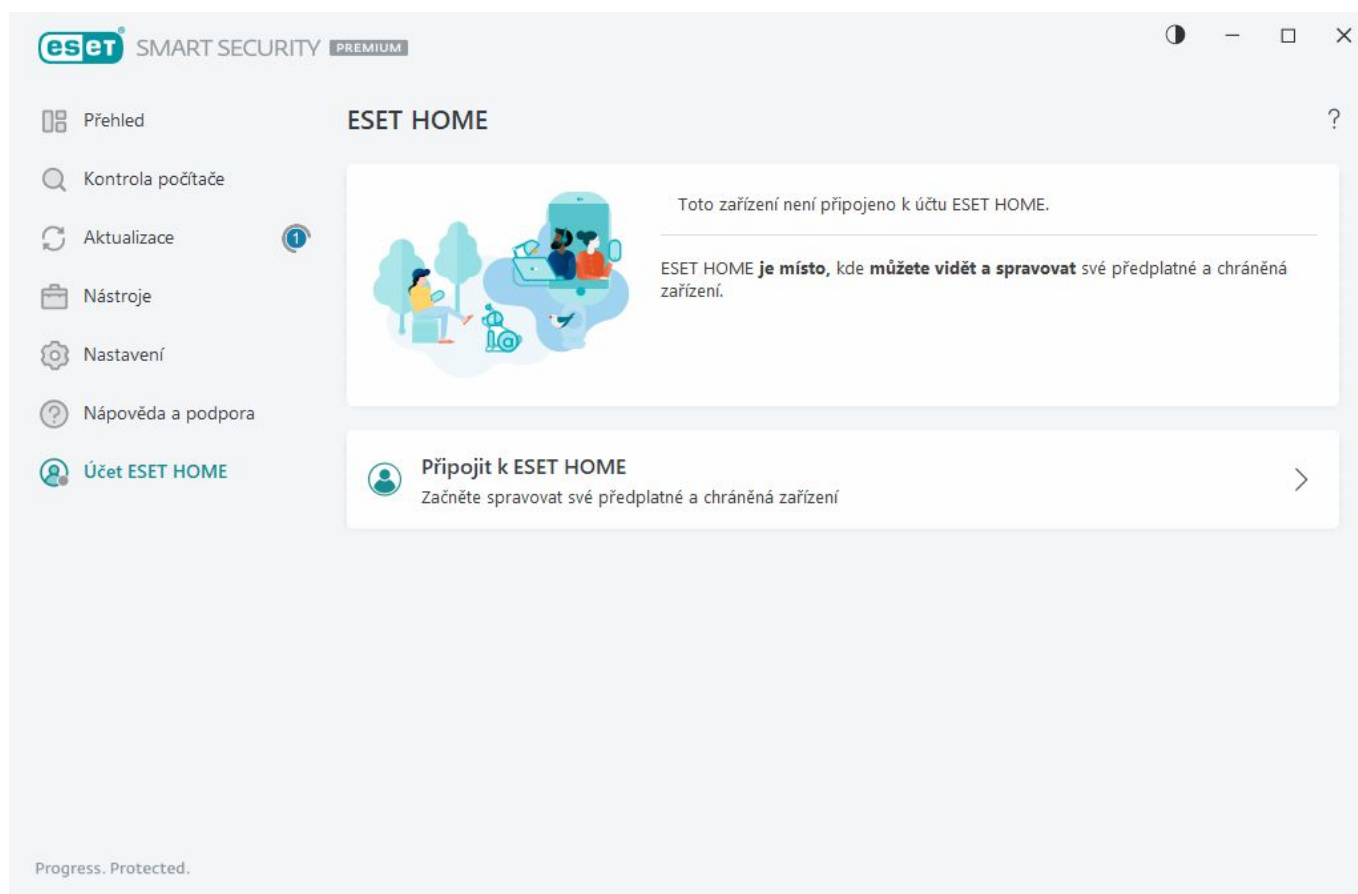
Základní informace pro technickou podporu – tuto možnost použijte, pokud po vás specialisté technické podpory vyžadují informace o vašem počítači (informace o předplatném, verzi produktu, operačním systému, atp.).

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

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

Účet ESET HOME

Zkontrolovat stav připojení k účtu ESET HOME můžete v [hlavním okně programu](#) > **Účet ESET HOME**.



Toto zařízení není připojeno k účtu ESET HOME.

Kliknutím na [Připojit k ESET HOME](#) připojíte své zařízení k [ESET HOME](#) a můžete spravovat své předplatné a chráněná zařízení. Můžete obnovit, upgradovat nebo prodloužit své předplatné a zobrazit důležité informace. Na portálu ESET HOME nebo v mobilní aplikaci můžete přidávat různá předplatná, stahovat produkty do svých zařízení, kontrolovat stav zabezpečení produktů nebo sdílet předplatné prostřednictvím e-mailu. Více informací naleznete v [Online nápovědě ESET HOME](#).

Toto zařízení je připojeno k účtu ESET HOME

Zabezpečení zařízení můžete spravovat na dálku pomocí [portálu ESET HOME](#) nebo stejnojmenné mobilní aplikace. Kliknutím na **App Store** nebo **Google Play** se zobrazí QR kód, který můžete naskenovat mobilním telefonem a stáhnout si mobilní aplikaci ESET HOME ze stejnojmenných obchodů s aplikacemi.

Účet ESET HOME – jméno vašeho účtu ESET HOME.

Název zařízení – název zařízení, pod jakým se bude zobrazovat v účtu ESET HOME.

Otevřít ESET HOME – otevře portál ESET HOME (portál pro správu licencí a připojených zařízení).

Chcete-li zařízení odpojit od účtu ESET HOME, klikněte na možnost **Odpojit od ESET HOME > Odpojit**. Předplatné použité pro aktivaci zůstane aktivní a vaše zařízení bude chráněno.

Připojení k ESET HOME

Pro zobrazení a správu předplatného, včetně aktivovaných zařízení, připojte zařízení k [ESET HOME](#). Můžete zobrazit důležité podrobnosti o předplatném, obnovit jej, prodloužit nebo přejít na vyšší úroveň předplatného. Na portálu ESET HOME nebo v mobilní aplikaci můžete přidávat různá předplatná, stahovat produkty do svých zařízení, kontrolovat stav jejich zabezpečení nebo sdílet předplatné prostřednictvím e-mailu. Více informací naleznete v [Online nápovědě ESET HOME](#).

Přihlášení k účtu ESET HOME

Přihlásit se pomocí Google

Přihlásit se pomocí Apple

Naskenovat QR kód

E-mailová adresa

Heslo

Zapomněli jste heslo?

Přihlásit se

Zrušit

Nemáte účet? [Vytvořte si jej!](#)

Pro připojení zařízení ke svému ESET HOME účtu:

Pokud se připojujete k účtu ESET HOME během instalace, nebo pro aktivaci vyberete možnost **Použít účet ESET HOME**, prostudujte si postup v kapitole [Použití účtu ESET HOME](#).

i Pokud již máte ESET Smart Security Premium nainstalovaný a aktivovaný pomocí předplatného přidaného k účtu ESET HOME, můžete své zařízení připojit k ESET HOME pomocí portálu ESET HOME. Více informací, jak ESET Smart Security Premium připojit, si prostudujte v kapitole produktové příručky [Přihlášení ke svému účtu ESET HOME](#) a [Přidání zařízení v ESET HOME](#).

1. V [hlavním okně programu](#) klikněte na Účet **ESET HOME** > **Připojit k ESET HOME**, případně v oznámení **Připojte toto zařízení k účtu ESET HOME** klikněte na odkaz **Připojit k ESET HOME**.

2. [Přihlaste se ke svému účtu ESET HOME](#).

i Pokud zatím nemáte účet ESET HOME, pro registraci nebo zobrazení instrukcí v [Online nápovědě ESET HOME](#) klikněte na tlačítko **Vytvořit účet**.

V případě, že si na heslo nemůžete vzpomenout, klikněte na možnost **Zapomněli jste heslo?** a pokračujte dle instrukcí v [Online nápovědě ESET HOME](#).

3. Zadejte **Název zařízení** a klikněte na možnost **Pokračovat**.

4. Po úspěšném připojení se zobrazí okno s podrobnostmi. Klikněte na **Hotovo**.

Přihlášení do ESET HOME

K účtu ESET HOME se přihlásíte pomocí jednoho z uvedených způsobů:

- **Pomocí e-mailové adresy a hesla k účtu ESET HOME** – Zadejte svou e-mailovou adresu a heslo, které jste použili při vytvoření účtu ESET HOME, a klikněte na tlačítko **Přihlásit se**.
- **Pomocí svého účtu Google/AppleID** – Klikněte na tlačítko **přihlášení prostřednictvím Google, případně Apple** a přihlaste se příslušným účtem. Po úspěšném přihlášení vás přesměrujeme na potvrzovací webovou stránku portálu ESET HOME. Pro pokračování klikněte zpět do produktu ESET. Další informace o přihlášení pomocí účtů Google/AppleID naleznete v [Online nápovědě k ESET HOME](#).
- **Naskenovat QR kód** – Kliknutím na příslušné tlačítko **zobrazíte QR kód** pro přihlášení. Otevřete si mobilní aplikaci ESET HOME a naskenujte QR kód, případně QR kód zaměříte fotoaparátem zařízení. Další informace naleznete v [Online nápovědě k ESET HOME](#).



Pokud zatím nemáte účet ESET HOME, pro registraci nebo zobrazení instrukcí v [Online nápovědě ESET HOME](#) klikněte na tlačítko **Vytvořit účet**.

V případě, že si na heslo nemůžete vzpomenout, klikněte na možnost **Zapomněli jste heslo?** a pokračujte dle instrukcí v [Online nápovědě ESET HOME](#).

[Neúspěšné přihlášení – běžné chyby.](#)

eSet SMART SECURITY PREMIUM

Přihlášení k účtu ESET HOME

Přihlásit se pomocí Google

Přihlásit se pomocí Apple

Naskenovat QR kód

eSet HOME

E-mailová adresa

Heslo

[Zapomněli jste heslo?](#)

Přihlásit se Zrušit

Nemáte účet? [Vytvořte si její!](#)

Neúspěšné přihlášení – běžné chyby

Nepodařilo se nám najít účet, který odpovídá zadané e-mailové adrese

Zadaná e-mailová adresa neodpovídá žádnému ESET HOME účtu. Po kliknutí na **Zpět** zadejte správnou e-mailovou adresu a heslo.

Abyste se mohli přihlásit, je třeba si vytvořit účet ESET HOME. Pokud ještě účet nemáte, klikněte na **Zpět** a dále vyberte možnost **Vytvořit účet**, případně si prostudujte v příručce k portálu ESET HOME kapitolu [Vytvoření nového účtu ESET HOME](#).

Uživatelské jméno a heslo se neshodují

Zadané heslo neodpovídá zadané e-mailové adrese. Klikněte na **Zpět**, zadejte správné heslo a ověřte správnost zadané e-mailové adresy. Pokud se stále nemůžete přihlásit, klikněte na **Zpět** a dále vyberte možnost **Zapomněl jsem heslo**, abyste mohli obnovit své heslo a postupujte podle pokynů na obrazovce. Případně si prostudujte v příručce k portálu ESET HOME kapitolu [Zapomněli jste heslo k účtu ESET HOME](#).

Vybraná možnost přihlášení neodpovídá vašemu účtu

Váš účet ESET HOME je propojen s účtem třetí strany. Pokud se chcete přihlásit do ESET HOME, klikněte na **Přihlásit se pomocí Google** nebo **Přihlásit se pomocí Apple** a k příslušnému účtu se přihlaste. Po úspěšném přihlášení vás přesměrujeme na potvrzovací webovou stránku portálu ESET HOME. Svůj účet třetí strany můžete odpojit od svého účtu ESET HOME na portálu ESET HOME.

Nesprávné heslo

K této chybě může dojít, pokud je váš ESET Smart Security Premium již připojen k ESET HOME a provádíte změny, které vyžadují přihlášení (například deaktivace Anti-Theft) a zadané heslo neodpovídá přihlašovacímu údajům k vašemu účtu. Po kliknutí na **Zpět** zadejte správné heslo. Pokud se stále nemůžete přihlásit, klikněte na **Zpět** a dále vyberte možnost **Zapomněl jsem heslo**, abyste mohli obnovit své heslo a postupujte podle pokynů na obrazovce. Případně si prostudujte v příručce k portálu ESET HOME kapitolu [Zapomněli jste heslo k účtu ESET HOME](#).

Přidání zařízení v ESET HOME

Pokud již máte ESET Smart Security Premium nainstalovaný a aktivovaný pomocí předplatného přidaného k účtu ESET HOME, můžete své zařízení připojit k ESET HOME pomocí portálu ESET HOME.

1. [Odešlete do zařízení žádost o připojení](#).
2. V ESET Smart Security Premium se zobrazí dialogové okno **Připojte toto zařízení k účtu ESET HOME** a názvem tohoto účtu. Kliknutím na **Povolit** se zařízení k účtu připojí.

i Pokud nedojde k žádné interakci, přibližně po 30 minutách bude žádost o připojení automaticky zrušena.

Rozšířená nastavení

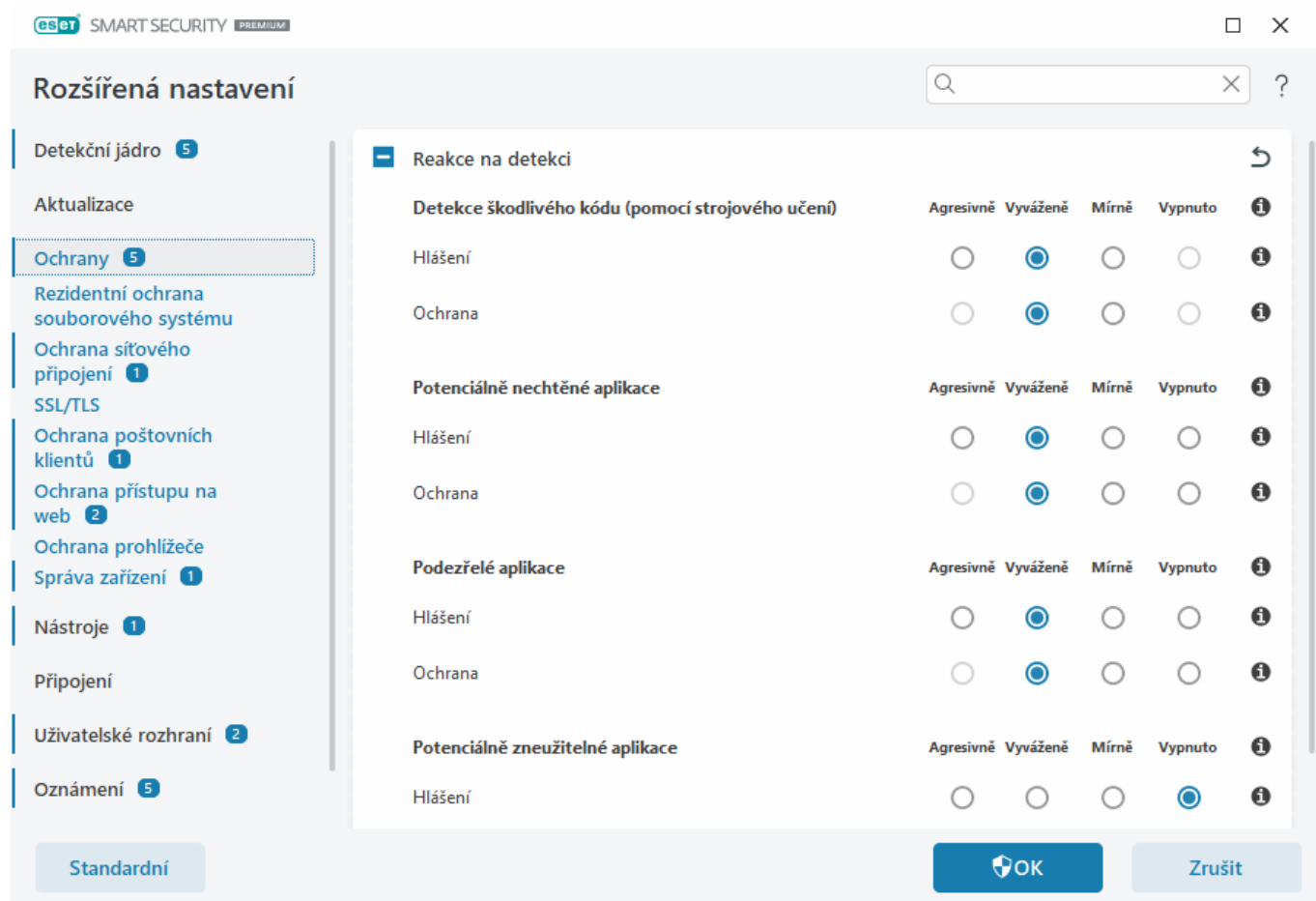
Rozšířená nastavení umožňují podrobné nastavení ESET Smart Security Premium podle vašich potřeb.

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

i V závislosti na [Přístupu k nastavení](#) můžete být vyzváni k zadání hesla pro otevření Rozšířených nastavení.

V rozšířených nastaveních můžete provádět následující nastavení:

- [Detekční jádro](#)
- [Aktualizace](#)
- [Ochrany](#)
- [Nástroje](#)
- [Připojení](#)
- [Uživatelské rozhraní](#)
- [Oznámení](#)
- [Nastavení ochrany soukromí](#)



Detekční jádro

[Rozšířená nastavení](#) > **Detekční jádro** umožňuje konfigurovat následující možnosti:

- [Výjimky](#)
- [Rozšířená nastavení](#)

- [Kontrola síťové komunikace](#)

Výjimky

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

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

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

Nezaměňujte mezi sebou jednotlivé typy výjimek:

- [Vyloučené procesy](#) – z kontroly budou vyloučeny všechny souborové operace přiřazené vyloučeným aplikačním procesům (to může být užitečné pro zvýšení rychlosti zálohování a dostupnosti služeb),
- [Vyloučené přípony souborů](#),
- [HIPS výjimky](#),
- [Filtr výjimek pro cloudovou ochranu](#).

Výkonnostní výjimky

Prostřednictvím výkonnostních výjimek můžete vyloučit soubory nebo složky z kontroly.

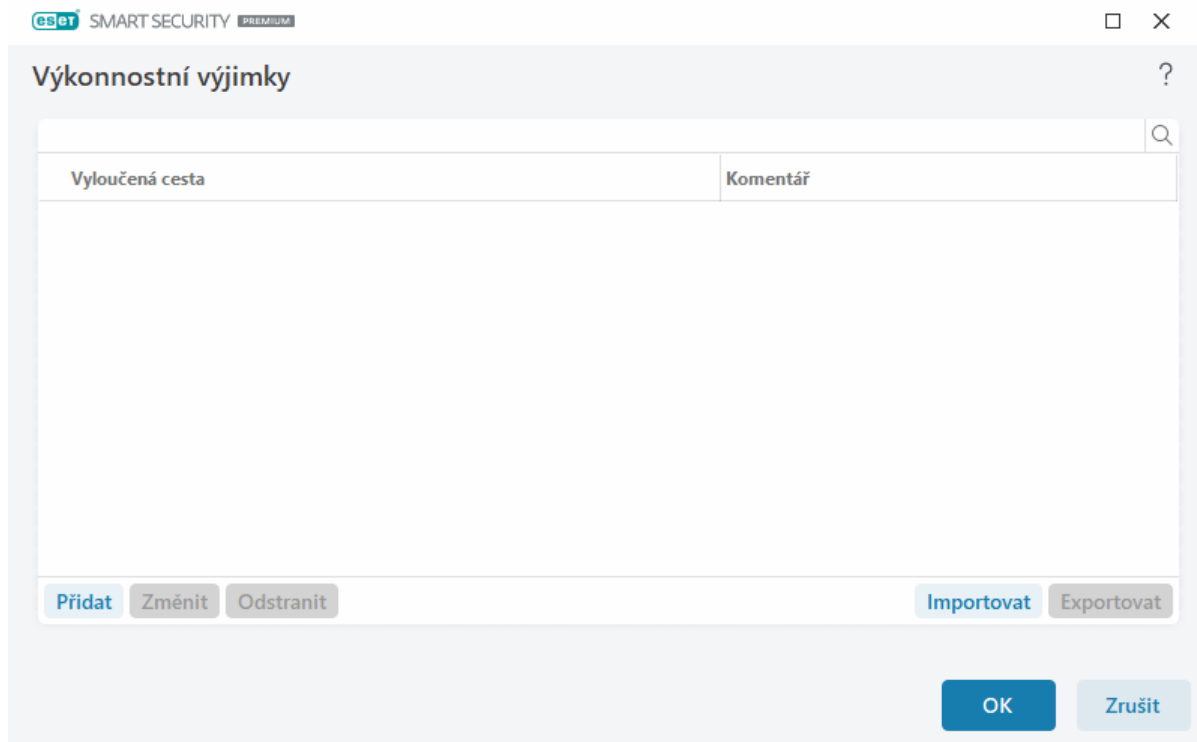
Pro zajištění kontroly všech objektů na výskyt hrozeb doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Příkladem, kdy je nutné vyloučit objekt z kontroly (například velké databázové soubory), je situace, kdy v průběhu kontroly dochází ke zpomalení počítače nebo konfliktu s právě používanou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

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



Nezaměňujte tuto funkci s [detekčními výjimkami](#), možností pro [vyloučení přípon souborů](#) z kontroly, možností pro tvorbu [HIPS výjimek](#) nebo [vyloučení procesů](#).

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



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

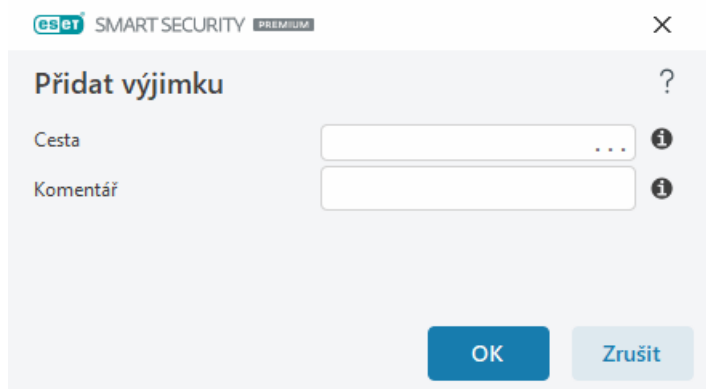
Ovládací prvky

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

Přidání a úprava výkonnostních výjimek

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

i **Cestu můžete zadat ručně nebo ji vybrat pomocí Průzkumníka**
Pro vybrání cesty klikněte na symbol ... v poli **Cesta**.
Pro více informací se podívejte do části [příklady formátů výjimek](#).



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

Formát výjimky

- 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.

Systémové proměnné ve výjimkách

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.

Zástupné znaky uprostřed cesty nejsou podporované



Důrazně nedoporučujeme používání zástupných znaků uprostřed cesty (například C:\Tools*\Data\file.dat), pokud to nevyžaduje infrastruktura systému.

V případě [detekčních výjimek](#) neexistují žádná omezení pro použití zástupných znaků uprostřed cesty.

Pořadí výjimek



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

Formát výjimky podle cesty

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

Formát výjimky

- 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.

Systémové proměnné ve výjimkách

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.

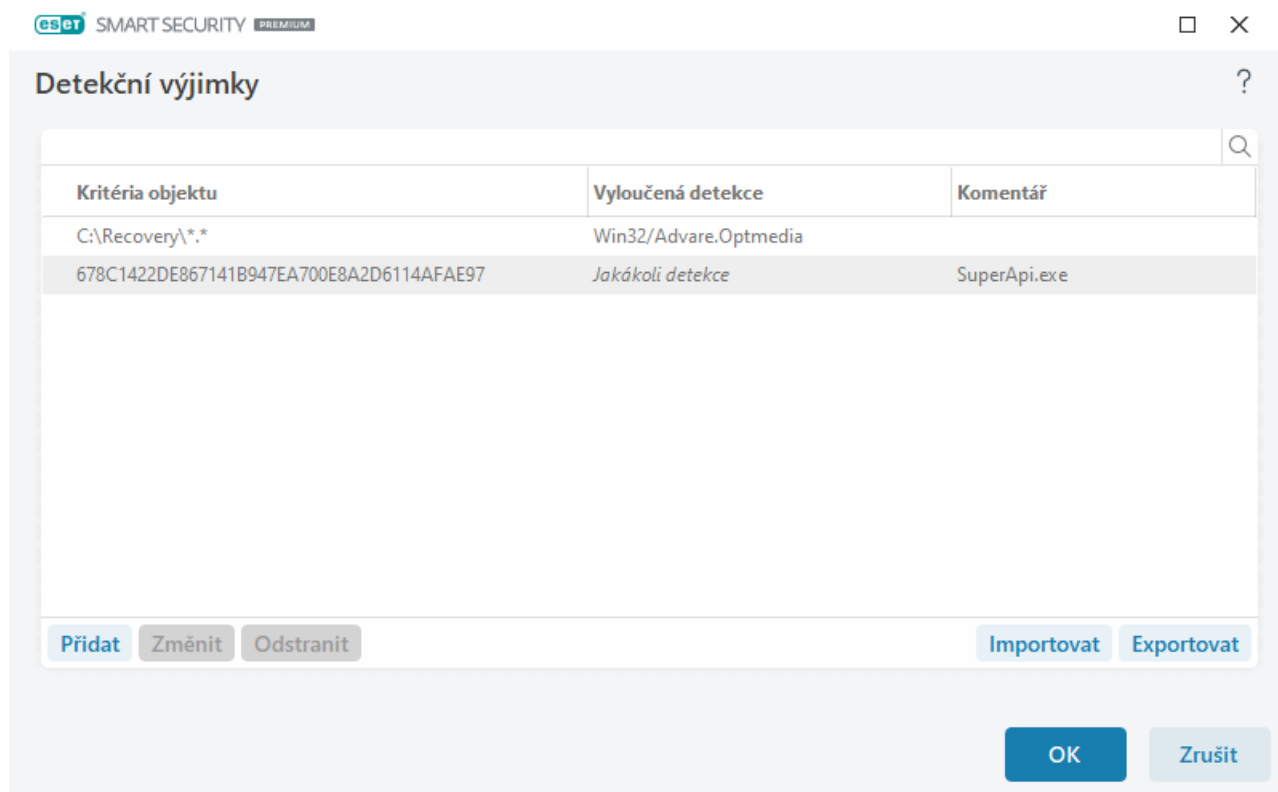
Detekční výjimky

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

Jak detekční výjimky fungují?

Detekční výjimky se nechovají stejně jako [výkonnostní výjimky](#), které slouží k vyloučení souborů nebo složek z kontroly. Objekt se vyloučí v případě, že je zachycen detekčním jádrem a vyhovuje některému z pravidel uvedených na seznamu detekčních výjimek.

Například podle prvního řádku dle obrázku níže bude z detekčního jádra vyloučen objekt detekovaný jako Win32/Adware.Optmedia, a může se nacházet v umístění *C:\Recovery\file.exe*. Dle druhého řádku bude soubor s uvedeným SHA-1 kontrolním součtem vyloučen bez ohledu na název detekce.



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

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

i Nezaměňujte tuto funkci s [výkonnostními výjimkami](#), možností pro [vyloučení přípon souborů](#) z kontroly, možností pro tvorbu [HIPS výjimek](#) nebo [vyloučení procesů](#).

Pro [vyloučení objektu](#) (na základě názvu detekce nebo kontrolního součtu 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

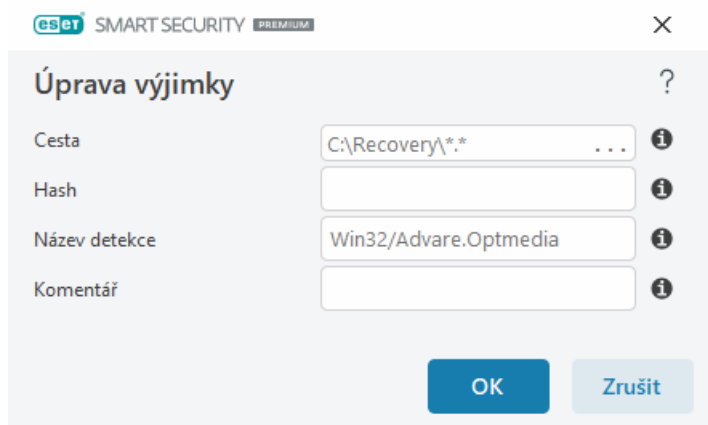
- **Cesta** – pomocí této možnosti můžete omezit, v případě potřeby, výjimku jen na konkrétní umístění.
- **Název detekce** – pokud je u vyloučeného souboru uveden i název [detekce](#), znamená to, že je soubor vyloučen pro danou detekci, nikoli celý. Pokud však bude soubor infikován později jiným malwarem, 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.

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 Smart Security Premium 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.

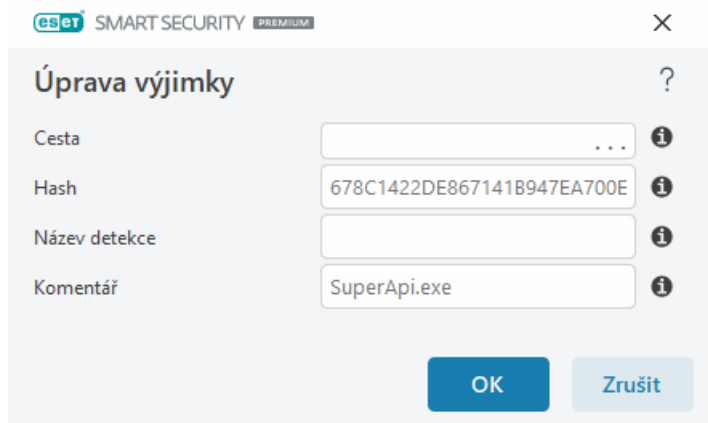
Další informace naleznete v kapitole [Formát výjimky podle cesty](#).



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.



Výjimky na základě názvu detekce

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 Smart Security Premium:
- @NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
 - @NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
 - @NAME=Win32/Bagle.D@TYPE=worm

Ovládací prvky

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

Průvodce vytvořením detekční výjimky

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

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

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

- **Konkrétní soubory** – pomocí této možnosti vyloučíte konkrétní soubor podle jeho SHA-1 kontrolního součtu.
- **Detekce** – vyloučí soubor podle názvu detekce.
- **Cesta + Detekce** – vyloučí soubory podle názvu detekce a cesty, včetně názvu souboru (např, `file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe`).

Na základě typu detekce je vždy předvybrána doporučená možnost.

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

Rozšířená nastavení detekčního jádra

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

Kontrola síťové komunikace

Kontrola síťové komunikace poskytuje ochranu před malwarem pro aplikační protokoly, která integruje několik pokročilých technik kontroly škodlivého kódu. Kontrola síťové komunikace automaticky kontroluje protokoly HTTP(S), POP3(S) a IMAP(S) bez ohledu na internetový prohlížeč nebo e-mailového klienta. Kontrolu síťové komunikace můžete zapnout nebo vypnout v [Rozšířených nastaveních](#) > **Detekční jádro** > **Kontrola síťové komunikace**.

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

- [Ochrana přístupu na web](#)
- [Rodičovské kontroly](#)
- [Ochrana soukromí a zabezpečení v prohlížeči](#)
- [Zabezpečené bankovníctví a prohlížení webu](#)
- [SSL/TLS](#)
- [Anti-Phishingová ochrana](#)
- [Ochrany poštovních klientů](#),

Cloudová ochrana

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

[ESET LiveGuard](#) je funkce, která přidává vrstvu cloudové ochrany speciálně navrženou pro snížení dopadu zcela nových hrozeb. Pokud je funkce zapnutá, podezřelé vzorky, které dosud nebyly potvrzené jako neškodné a mohou potenciálně obsahovat škodlivý kód, jsou přesunuté do cloudu společnosti ESET.

K dispozici jsou následující možnosti:

Zapnout reputační systém ESET LiveGrid®, systém zpětné vazby ESET LiveGrid® a ESET LiveGuard

Reputační systém ESET LiveGrid® porovnává soubory v cloudu oproti neškodnému nebo škodlivému chování souborů. Systém zpětné vazby ESET LiveGrid® sbírá informace, které se mohou týkat vašeho počítače v souvislosti s nově detekovanými hrozbami. Funkce ESET LiveGuard detekuje v sandboxu nové a dosud neznámé hrozby pomocí analýzy jejich chování.

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®. Proaktivní ochrana ESET LiveGuard blokuje nové soubory před spuštěním až do doby, než je hotová analýza jejich škodlivosti.

Zapnout reputační systém 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®.

Zapnout systém zpětné vazby ESET LiveGrid®

Reputační systém ESET LiveGrid® a systém zpětné vazby ESET LiveGrid® shromažďuje z vašeho počítače pouze informace, které se týkají nové infiltrace. To může zahrnovat:

- Vzorek nebo kopii souboru, ve kterém se hrozba objevila
- Cesty k umístění souboru
- Název souboru
- Datum a čas
- Způsob, jakým se hrozba dostala do počítače
- Informace o stavu zabezpečení počítače

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



Více informací o zasílaných datech naleznete v dokumentu [Zásady ochrany osobních údajů](#).

Můžete se rozhodnout ESET LiveGrid® nezapínat

Nepřijdete tím o žádnou funkci, ale v některých případech může ESET Smart Security Premium reagovat na nové hrozby se zpožděním, než kdyby byl ESET LiveGrid® aktivní. 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.

i Více informací o technologii ESET LiveGrid® naleznete ve [slovníku pojmů](#).
Názorné ukázky, jak zapnout nebo vypnout ESET LiveGrid® v produktu ESET Smart Security Premium máme k dispozici v Databázi znalostí v angličtině a několika dalších jazycích.

Konfigurace cloudové ochrany v Rozšířených nastaveních

Chcete-li získat přístup k nastavení pro ESET LiveGrid® a ESET LiveGuard, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Cloudová ochrana**.

- **Zapnout reputační systém ESET LiveGrid® (doporučeno)** – reputační systém ESET LiveGrid® zvyšuje účinnost anti-malwarových řešení ESET ověřováním souborů vůči cloudové databázi povolených a zakázaných souborů.
- **Zapnout systém zpětné vazby ESET LiveGrid®** – odesílá příslušná data (popsaná v sekci **Odeslání vzorků** níže) spolu s informacemi o pádech a statistikami do ESET Research Lab k další analýze.
- **Zapnout ESET LiveGuard** – ESET LiveGuard zajišťuje další vrstvu ochrany využitím sandboxu k analyzování a detekci dosud neznámých hrozeb. ESET LiveGuard je možné zapnout pouze v případě, kdy je aktivní ESET LiveGrid®.
- **Odesílat informace o pádech a diagnostická data** – po aktivování ESET LiveGrid® se budou odesílat diagnostická data, jako jsou informace o pádech a výpisy obsahu paměti jednotlivých modulů. Doporučujeme ponechat tuto funkci zapnutou, abyste pomohli firmě ESET diagnostikovat problémy, vylepšovat produkty a zajistit lepší ochranu uživatelů.
- **Odesílat anonymní statistiky** – tímto umožníte společnosti ESET shromažďovat informace o nově detekovaných hrozbách, jako je název hrozby, datum a čas detekce, metoda detekce a přidružená metadata, verze produktu a konfigurace včetně informací o vašem systému.
- **Kontaktní e-mail (nepovinný údaj)** – zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.

Odesílání vzorků

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

Automatické odesílání detekovaných vzorků

Vyberte, jaké druhy vzorků budete odesílat společnosti ESET k analýze a k vylepšení budoucí detekce (výchozí maximální velikost vzorku je 64 MB). K dispozici jsou následující možnosti:

- **Všechny detekované vzorky** – Všechny [objekty](#) detekované [Detekčním jádrem](#) (včetně potenciálně nechtěných aplikací, pokud jsou v nastavení skeneru povoleny).
- **Všechny vzorky kromě dokumentů** – všechny detekované objekty kromě **Dokumentů** (viz níže).

- **Neodesílat** – Detekované objekty nebudou společností ESET odeslány.

Automatické odesílání podezřelých souborů

Tyto vzorky budou rovněž posílány společnosti ESET i v případě, že nebudou detekovány detekčním jádrem. Například vzorky, které se vyhnuly detekci těsně, nebo je některý z [modulů ochrany](#) ESET Smart Security Premium považuje za podezřelý, případně vykazují nejasné chování (výchozí maximální velikost vzorku je 64 MB).

- **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. Zapnutím této možnosti zlepšuje globální detekci spamu, včetně zlepšení detekce spamu v budoucnosti.
- **Odstranit ze serverů společnosti ESET spustitelné soubory, archivy, skripty, další vzorky a zprávy označené jako pravděpodobný spam** – pomocí rozbalovacího menu se rozhodněte, po jaké době se mají odstranit vzorky odeslané k analýze do ESET LiveGuard.
- **Dokumenty** – zahrnují dokumenty Microsoft Office nebo PDF s aktivním obsahem nebo bez něj.
- **Odstranit dokumenty ze serverů společnosti ESET** – pomocí rozbalovacího menu se rozhodněte, po jaké době se mají odstranit dokumenty odeslané k analýze do ESET LiveGuard.

✓ [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.

✓ Chcete-li vyloučit soubory stažené z webu `download.domain.com`, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Cloudová ochrana** > **Odesílání vzorků** a klikněte na **Změnit** vedle položky **Výjimka**. Na řádku **Výjimky** klikněte na **Změnit** a v zobrazeném dialogovém okně a definujte výjimku následovně: `.download.domena.cz`.

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

[ESET LiveGuard](#)

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.domena.cz přejděte v [Rozšířených nastaveních](#) do sekce **Detekční jádro > Cloudová ochrana > Odesílání vzorků**. Na řádku **Výjimky** klikněte na Změnit a v zobrazeném dialogovém okně definujte výjimku následovně: *download.domena.cz*.

ESET LiveGuard

ESET LiveGuard je funkce, která přidává vrstvu [cloudové ochrany](#) speciálně navrženou pro snížení dopadu zcela nových hrozeb

Pokud je funkce zapnutá, podezřelé vzorky, které dosud nebyly potvrzené jako neškodné a mohou potenciálně obsahovat škodlivý kód, jsou přesunuté do cloudu společnosti ESET. Odeslané vzorky spouštíme v sandboxu a vyhodnocujeme za pomoci pokročilých modulů detekčního jádra. Škodlivé vzorky nebo podezřelá nevyžádaná pošta (spam) jsou odeslány do ESET LiveGrid®. Přílohy e-mailů jsou zpracovávány samostatně a podléhají odeslání do ESET LiveGuard. [Rozsah odeslaných souborů a dobu uchovávání souboru v cloudu ESET](#) můžete nastavit. Dokumenty a soubory PDF s aktivním obsahem (makra, javascript) nejsou ve výchozím nastavení odesílány.

ESET LiveGuard můžete zapnout nebo vypnout:

- V [hlavním okně programu](#) na záložce **Nastavení > Ochrana počítače**
- V [Rozšířených nastaveních](#) > **Detekční jádro > Cloudová ochrana**

K rozšířeným nastavením pro ESET LiveGuard se dostanete z [Rozšířená nastavení](#) > **Cloudová ochrana > ESET LiveGuard**.

Akce při detekci – nastaví akci, kterou funkce provede v případě, kdy je analyzovaný vzorek vyhodnocený jako hrozba.

Proaktivní ochrana – povoluje nebo blokuje spuštění souborů, které jsou v ten moment analyzovány funkcí ESET LiveGuard. Pokud je soubor podezřelý, proaktivní ochrana zablokuje jeho spuštění až do dokončení analýzy. Proaktivní ochrana detekuje soubory pouze případech, kdy byly:

- stažené pomocí podporovaného webového prohlížeče
- stažené z poštovního klienta
- vybalované z nešifrovaných i šifrovaných archivů prostřednictvím podporovaných nástrojů pro práci s archivy
- spuštěné a otevřené z výměnných médií

Podporované aplikace naleznete v tabulce níže:

Webové prohlížeče	Poštovní klienti	Nástroje pro práci s archivy	Výměnná média
Internet Explorer	Microsoft Outlook	WinRAR	USB flash disk
Microsoft Edge	Mozilla Thunderbird	WinZIP	Externí harddisk (USB)
Chrome	Microsoft Mail	Kontextová možnost Extrahovat v Průzkumníku	CD/DVD,
Firefox		7zip	Disketa
Opera			Vestavěná čtečka čipových karet
Prohlížeč Brave			






Poznámka

i Protože ESET Smart Security Premium klasifikuje `explorer.exe` jako archivační program, přenášení souborů z vyloučeného umístění do chráněného je kopírováním přes schránku Průzkumníku Windows proaktivní ochranou blokováno.

i Pokud je Proaktivní ochrana nastavena na **Blokovat spuštění do obdržení výsledku analýzy** a chcete povolit používání analyzovaného souboru, klikněte pravým tlačítkem myši na soubor > **Odblokovat soubory analyzované prostřednictvím ESET LiveGuard**.

Maximální doba čekání na výsledek analýzy (v min.) – v této části můžete nastavit, za jak dlouho má být povoleno používání souboru, nehlédě na tom, zda došlo k dokončení analýzy, či ne.

ESET LiveGuard vás bude informovat o stavu analýzy pomocí oznámení. Podívejte se níže, jak taková oznámení vypadají:

Titulek oznámení	Popis
 Přístup k souboru je blokován z důvodu analýzy	Soubor je blokován ESET LiveGuard. ESET LiveGuard provádí analýzu pro ověření, zda je bezpečné soubor spouštět. Můžete chvíli počkat nebo zvolit jednu z následujících možností: <ul style="list-style-type: none"> • Povolit přístup k souboru – pomocí této možnosti odblokujete analyzovaný soubor. Analýza stále probíhá a o výsledku kontroly budete informováni. Tuto akci nedoporučujeme, pokud si nejste jisti autentičností souboru. • Změnit nastavení – kliknutím si zobrazíte nastavení ochrany počítače, ve kterém můžete vypnout ESET LiveGuard a jeho proaktivní ochranu.
 Soubor je možné používat	Soubor již není blokován. Analýza pokračuje a po ukončení analýzy obdržíte oznámení o výsledku. Soubor můžete otevřít.
 Stále probíhá analýza souboru	ESET LiveGuard potřebuje více času na dokončení analýzy. V případě potřeby můžete soubor otevřít.
 Hrozba byla odstraněna	ESET LiveGuard dokončil analýzu. Soubor byl vyléčen od nalezené hrozby.
 Soubor je bezpečný	ESET LiveGuard dokončil analýzu. Soubor je bezpečný k použití.

Pokud ESET LiveGuard nefunguje správně, v [hlavním okně programu](#) na záložce **Přehled** se zobrazí související oznámení. Pro vyřešení problému postupujte podle kroků uvedených v oznámení. V případě přetrvávajících potíží kontaktujte [technickou podporu společnosti ESET](#).

Detekce škodlivého kódu

Sekce **Detekce škodlivého kódu** je přístupná z [Rozšířených nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** a umožňuje konfigurovat parametry pro profily kontroly.

Volitelná kontrola

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

Po výběru profilu kontroly můžete nakonfigurovat následující možnosti:

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

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

ThreatSense – možnosti rozšířených nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Profily kontroly

K dispozici jsou čtyři předdefinované profily kontroly ESET Smart Security Premium:

- **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.
- **Hlubková kontrola počítače:** Profil hloubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.
- **Kontrola počítače:** Toto je výchozí profil používaný při standardní kontrole počítače.

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

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



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

Cíle kontroly

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

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

Další cíle kontroly si můžete vybrat ve stromové struktuře.

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

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

Kontrola při nečinnosti

Kontrolu při nečinnosti můžete nastavit v [Rozšířených nastaveních](#) v sekci **Detekční jádro > Detekce škodlivého kódu > Kontrola při nečinnosti**.

Kontrola při nečinnosti

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

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

nastaveních.

V Rozšířených nastaveních přepínačem aktivujte možnost **Zapisovat do protokolu**, pokud chcete průběh kontroly zapisovat do sekce [Protokoly](#) (v [hlavním okně programu](#) klikněte na **Nástroje > Protokoly** a z rozbalovacího menu **Detekce** vyberte možnost **Kontrola počítače**).

Detekce stavu nečinnosti

Více informací o možnostech definování akce, při které se spustí kontrola, naleznete v kapitole [Detekce stavu nečinnosti](#).

ThreatSense – možnosti rozšířených nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Detekce stavu nečinnosti

Nastavení Detekce stavu nečinnosti můžete konfigurovat v části [Rozšířená nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Kontrola při nečinnosti** > **Detekce stavu nečinnosti**. Tato nastavení určují spouštění [Kontroly při nečinnosti](#):

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

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

Kontrola po startu

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

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

ThreatSense – možnosti rozšířených nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Automatická kontrola souborů spouštěných při startu počítače

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

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

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

Mezi tyto možnosti patří také tyto dvě:

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

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

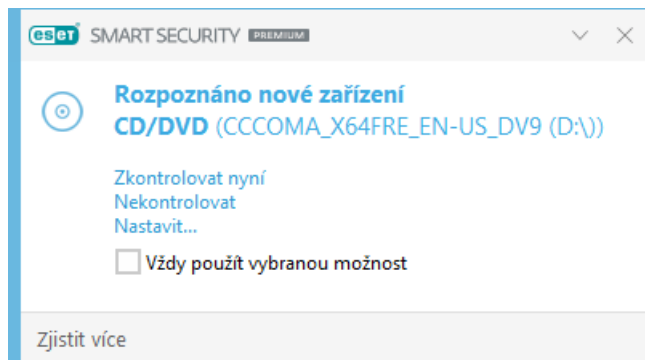
Priorita kontroly – definujte úroveň priority, při které se spustí kontrola počítače:

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

Výměnná média

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

Pokud je vloženo výměnné médium a v [Rozšířených nastaveních](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média** je nastavena možnost **Zobrazit možnosti kontroly**, objeví se následující dialogové okno:



Možnosti tohoto dialogu:

- **Zkontrolovat nyní** – spustí se ruční kontrola výměnného média.
- **Nekontrolovat** – po vybrání této možnosti se výměnné médium nekontroluje.
- **Nastavení** – otevře [Rozšířená nastavení](#).
- **Vždy použít vybranou možnost** – pokud vyberete toto pole, při příštím připojení výměnného média se provede stejná akce.

Kromě toho Správa zařízení ESET Smart Security Premium disponuje pokročilými funkcemi, které vám umožňují definovat pravidla pro zacházení s externími zařízeními připojovanými k vašemu počítači. Více informací naleznete v kapitole [Správa zařízení](#).

K přístupu do nastavení kontroly výměnných médií otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média**.

Akce po vložení vyměnitelného média – Vyberte výchozí akci, která bude provedena po vložení vyměnitelného média do počítače (CD/DVD/USB). Po vložení výměnného média do počítače vyberte požadovanou akci:

- **Nekontrolovat** – neprovede se žádná akce a upozornění **Nalezeno nové nařízení** se nezobrazí.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí kontrola jeho obsahu.
- **Zobrazit možnosti kontroly** – otevře možnost **Nastavení výměnných médií**.

Ochrana dokumentů

Modul ochrany dokumentů zajišťuje kontrolu dokumentů Microsoft Office před jejich otevřením a také kontroluje automaticky stahované soubory pomocí Internet Explorer, jako například prvky Microsoft 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 [Rozšířených nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Ochrana dokumentů** a klikněte na přepínač vedle **Zapnout ochranu dokumentů**.

ThreatSense – možnosti rozšířených nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).



Tento modul pracuje pouze s aplikacemi, které podporují rozhraní Microsoft Antivirus API (například Microsoft Office 2000 a novější nebo Microsoft Internet Explorer 5.0 a novější).

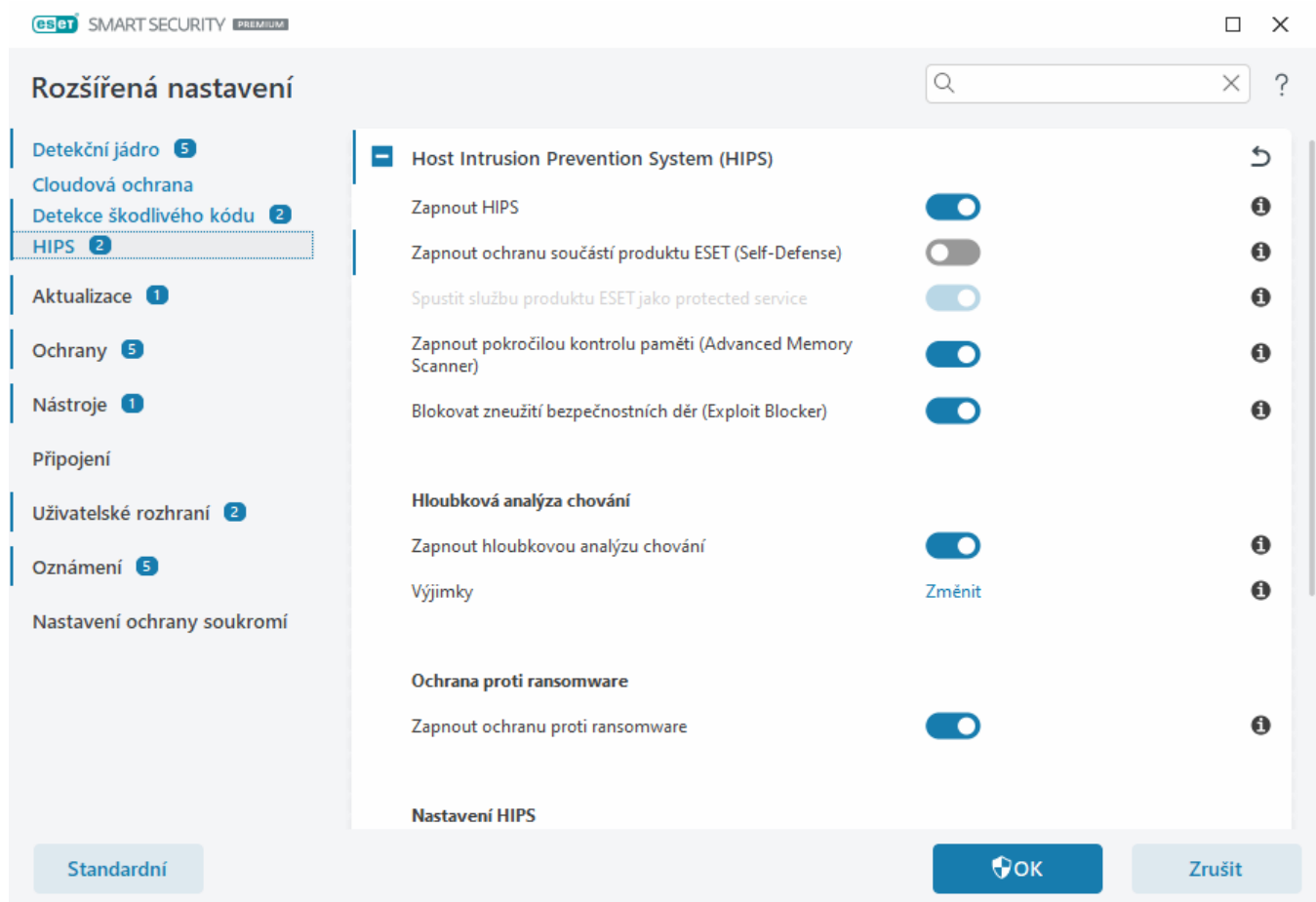
HIPS – Host Intrusion Prevention System



Pokud nejste zkušený uživatel, nedoporučujeme měnit nastavení systému HIPS. Chybnou úpravou nastavení HIPS se může systém stát nestabilní.

HIPS (Host-based Intrusion Prevention System) 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.

Systém HIPS můžete nastavit v [Rozšířených nastaveních](#) > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)**. Stav modulu HIPS je zobrazen v [hlavním okně programu](#) ESET Smart Security Premium > **Nastavení** > **Ochrana počítače**.



Host Intrusion Prevention System (HIPS)

Zapnout HIPS – HIPS je v ESET Smart Security Premium standardně zapnutý. Jeho vypnutím zakázete běh dalších součástí HIPS jako je například Exploit Blocker.

Zapnout ochranu součástí produktu ESET (Self-Defense) – ESET Smart Security Premium 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.

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.

Zapnout pokročilou kontrolu paměti (Advanced Memory Scanner) – tato funkce v kombinaci s blokováním zneužití bezpečnostních děr (Exploit Blocker) poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve [slovníku pojmů](#).

Blokovat zneužití bezpečnostních děr (Exploit Blocker) – tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, PDF čtečky a komponenty Microsoft Office). Tato funkce je standardně zapnuta. Více informací o této vrstvě ochrany naleznete ve [slovníku pojmů](#).

Hloubková analýza chování

Hloubková analýza chování je další vrstvou ochrany funkce HIPS. Toto rozšíření analyzuje chování běžících programů a varuje vás, jestliže jejich chování bude pro váš počítač škodlivé.

[HIPS výjimky Hloubkové analýzy chování](#) umožňují vyloučit procesy z kontroly. Pro zajištění všech kontrol na možné hrozby doporučujeme vytvářet vyloučení pouze v případě, že je absolutně nezbytné.

Ochrana proti ransomware

Zapnout ochranu proti ransomware – tato součást představuje další vrstvu funkce HIPS. Pro správnou funkci ochrany proti ransomware je třeba mít zapnutý Reputační systém ESET LiveGrid®. Více informací o tomto typu ochrany naleznete ve [slovníku pojmů](#).

Zapnout Intel® Threat Detection Technology – technologie pomáhá odhalovat útoky ransomwaru využitím unikátní telemetrie z procesoru Intel. Zvyšuje účinnost detekce, snižuje počet falešných poplachů a rozšiřuje možnosti zachycení pokročilých technik na obcházení detekce v paměti zařízení. Viz [podporované procesory](#).

Nastavení HIPS

HIPS může běžet v jednom z následujících **režimů**:

Režim filtrování	Popis
Automatický režim	Operace budou povoleny s výjimkou blokových 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.

Režim filtrování	Popis
Učící režim	Operace jsou povoleny a po každé operaci je vytvořeno pravidlo. Pravidla vytvořená v tomto režimu jsou viditelná v editoru Pravidel HIPS , ale jejich priorita je nižší než priorita pravidel vytvořených ručně nebo pravidel vytvářených v automatickém režimu. Vyberete-li v rozbalovací nabídce Režim filtrování možnost Učící režim , zpřístupní se nastavení Učící režim bude ukončen . Vyberte časové období (max. 14 dní), pro které bude učící režim aktivní. Po uplynutí zadaného období budete vyzváni k úpravě pravidel vytvořených pomocí HIPS v učícím režimu. Můžete také zvolit jiný režim filtrování nebo odložit rozhodnutí a pokračovat v používání režimu učení.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte režim filtrování, který se automaticky nastaví po ukončení běhu učícího režimu. Pokud vyberete možnost **Dotázat se uživatele**, pro změnu režimu filtrování modulu HIPS bude vyžadováno oprávnění administrátora.

Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům firewallu. Kliknutím na **Změnit** vedle položky **Pravidla** otevřete editor **Pravidla HIPS**. Zde můžete pravidla prohlížet, vytvářet nová, upravovat nebo odstranit stávající. Více detailů o vytváření pravidel a operacích HIPS naleznete v kapitole [Úprava pravidla HIPS](#).

HIPS výjimky

Prostřednictvím výjimek můžete vyloučit procesy z HIPS Hlubkové analýzy chování.

Chcete-li upravit výjimky pro HIPS, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)** > **Výjimky** > **Změnit**.



Nezaměňujte tuto funkci s možností pro [vyloučení přípon souborů](#) z kontroly, tvorbu [detekčních výjimek](#), [výkonnostních výjimek](#), [vyloučených procesů](#).

Pro vyloučení objektu z kontroly klikněte na tlačítko **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury. Existující výjimky můžete upravovat, případně odstranit.

Rozšířená nastavení HIPS

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

[Automaticky povolené ovladače](#) – seznam ovladačů, které budou vždy načteny, bez ohledu na nastavený režim filtrování, pokud nejsou blokovány uživatelským pravidlem.

Zapisovat všechny zablokované operace do protokolu – všechny zablokované operace se zapíší do protokolu HIPS. Tuto možnost aktivujte výhradně na výzvu specialisty technické podpory ESET. Mějte na paměti, že se následně začne generovat velké množství dat a může dojít ke zpomalení počítače.

Upozornit na změny v seznamu aplikací automaticky 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 – Odstranit ovladač ze seznamu.

Reset – obnoví seznam na výchozí hodnoty.

i Po kliknutí na tlačítko **Obnovit** vymažete všechny ovladače, které jste přidali ručně. V seznamu zůstanou pouze systémové ovladače.

i Po instalaci je seznam ovladačů prázdný. ESET Smart Security Premium je časem automaticky doplní.

Interaktivní režim HIPS

Přímo z okna HIPS oznámení můžete vytvořit pravidlo na základě akce, které modul HIPS detekoval, a definovat podmínky, za kterých bude tato operace povolena nebo blokována.

Pravidla vytvořená z oznámení jsou ekvivalentní ručně vytvořeným. Pravidlo vytvořené z oznámení může být však méně specifické, než pravidlo vytvořené prostřednictvím editoru pravidel. To znamená, že po vytvoření pravidla prostřednictvím editoru může stejná operace vyvolat zobrazení oznámení. Pro více informací si nastudujte [prioritu HIPS pravidel](#).

Pokud je jako výchozí akce pro pravidlo nastavena možnost **Vždy se dotázat**, dialogové okno se zobrazí při každé aktivaci pravidla. Následně se rozhodnete, 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 dotázáni.

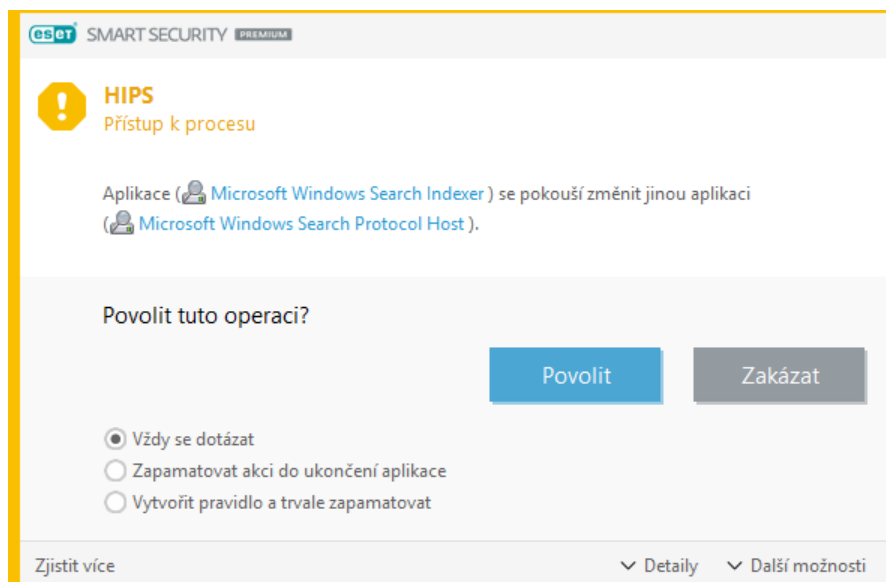
Nastavení detailních parametrů si zpřístupníte kliknutím na **Rozšířená nastavení**. Níže uvedené možnosti jsou dostupné v případě, kdy vyberete možnost **Vytvořit pravidlo a trvale zapamatovat**.

- **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/aplikací/registrem. [Pro více informací se podívejte na popis všech HIPS operací.](#)
- **Pouze pro cíl** – vyberte, zda bude pravidlo platné pro soubor/aplikaci/registr.

Již nechcete zobrazovat HIPS oznámení?

- ! Pro ukončení zobrazování oznámení přepněte režim filtrování na **Automaticky** v [Rozšířených nastaveních](#) > **Detekční jádro > HIPS > Host Intrusion Prevention System (HIPS).**



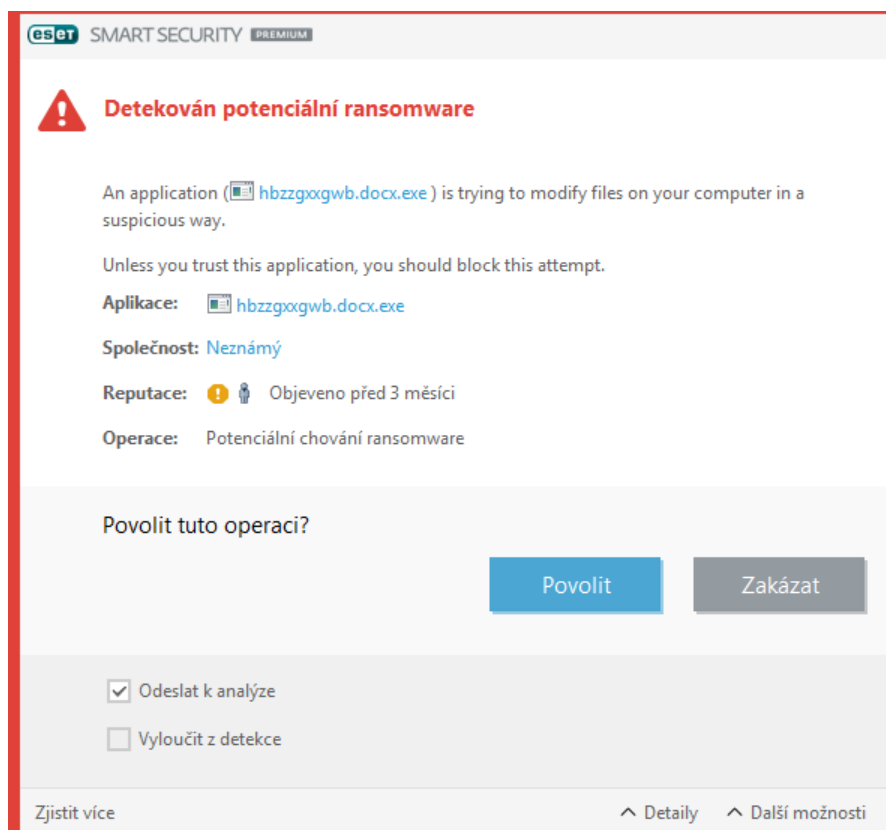
Učící režim skončil

Učící režim automaticky vytváří a ukládá pravidla. Všechna vytvořená pravidla můžete zkontrolovat v [nastavení pravidla HIPS](#). Tento režim je nejvhodnější pro počáteční konfiguraci systému HIPS, ale měl by být zapnutý jen krátkou dobu. Vytvoření pravidel proběhne bez interakce uživatele, protože ESET Smart Security Premium pravidla vytvoří na základě předem definovaných parametrů. Přepněte do **interaktivního** nebo **administrátorského režimu** až po vytvoření všech pravidel pro požadované procesy spuštěné v operačním systému, abyste předešli bezpečnostním rizikům.

Pokud nechcete nastavení měnit, můžete toto rozhodnutí odložit.

Detekován potenciální ransomware

Toto dialogové okno se zobrazí, pokud je detekována aplikace, jejíž chování je velmi podobné ransomware. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**.



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

! Pro fungování [ochrany proti ransomware](#) je vyžadována aktivní technologie ESET LiveGrid®.

Správa HIPS pravidel

V tomto dialogovém okně naleznete uživatelsky a automaticky vytvořená pravidla modulu HIPS. Více informací o vytváření HIPS pravidel naleznete v kapitole [Úprava pravidla HIPS](#). Podívejte se rovněž do kapitoly [Obecné principy HIPS](#).

Sloupce

Pravidlo – uživatelský nebo automaticky zadaný název pravidla.

Zapnuto – deaktivujte tuto možnost, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Zdroje – pravidlo se uplatní, pouze pokud událost vyvolají dané aplikace.

Cíle – pravidlo se použije, pouze pokud se operace týká daného cíle (souboru, aplikace nebo záznamu v registru).

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do [protokolu HIPS](#).

Oznámit – pokud je spuštěna událost, zobrazí se v pravém dolním rohu obrazovky oznámení.

Ovládací prvky

Přidat – kliknutím vytvoříte nové pravidlo.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odstraníte vybraný záznam.

Priorita pravidel HIPS

Neexistují žádné možnosti nastavení priority pravidel HIPS pomocí tlačítek nahoru/dolu (jako u [pravidel firewallu](#), kde se pravidla provádějí shora dolů).

- Všechna pravidla mají stejnou prioritu
- Specifičtější pravidla mají vyšší prioritu (například pravidlo pro konkrétní aplikaci je nadřazeno pravidlu platnému pro všechny aplikace)
- Interně HIPS obsahuje několik předdefinovaných pravidel s nejvyšší prioritou, která nemůžete ovlivnit (například nemůžete přepsat Self-Defense pravidla)
- Vámi vytvořená pravidla, která mohou způsobit zamrznutí systému, se nebudou aplikovat (budou mít nejnižší prioritu)

Úprava pravidla HIPS

Nejprve si prosím přečtěte kapitolu [Správa HIPS pravidel](#).

Název pravidla – uživatelský nebo automaticky zadaný název pravidla.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Operace ovlivní – vyberte typ operace, pro kterou má být pravidlo platné. Konkrétní pravidlo je možné použít pouze pro jeden typ operace nad vybraným cílem.

Zapnuto – deaktivujte tuto možnost pomocí přepínače, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do [protokolu HIPS](#).

Upozornit uživatele – 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** zadejte je ručně, případně po kliknutí na **Otevřít Editor registru** můžete přímo vybrat jednotlivé klíče z registru. 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.

Popis důležitých operací:

Operace se soubory

- **Vymazat soubor** – aplikace žádá o povolení vymazat cílový soubor.
- **Zápis do souboru** – aplikace žádá o povolení zapisovat do cílového souboru.
- **Přímý přístup na disk** – aplikace se snaží číst nebo zapisovat na disk nestandardním způsobem, který obchází běžné procedury Windows. Výsledkem může být změna souboru bez použití příslušného pravidla. Tato operace může být způsobena škodlivým kódem, který se snaží vyhnout se detekci, zálohovacím programem, který kopíruje celý obsah pevného disku nebo správcem oddílů který reorganizuje diskové oddíly.
- **Nainstalovat globální hook** – volání funkce SetWindowsHookEx z MSDN knihovny pomocí dané aplikace.
- **Načíst ovladač** – instalace a načítání ovladače do systému.

Operace aplikace

- **Ladění jiné aplikace** – připojení debuggeru k procesu. Při debuggingu můžete sledovat a měnit chování aplikace a přistupovat k jejím datům.
- **Zachytávat události jiné aplikace** – zdrojová aplikace se pokouší zachytit události cílové aplikace (například pokud se keylogger snaží zachytit aktivitu webového prohlížeče).
- **Ukončit/přerušit jinou aplikaci** – pozastavení, obnovení nebo ukončení procesu (může být vyvoláno přímo ze Správce úloh nebo ze záložky Procesy).
- **Spustit novou aplikaci** – spuštění nové aplikace nebo procesu.
- **Změnit stav jiné aplikace** – zdrojová aplikace se pokouší zapisovat do paměti cílové aplikace, případně se snaží spustit kód pod jejím jménem. Tato funkce je užitečná pro ochranu důležité aplikace, pokud ji nastavíte jako cílovou aplikaci v pravidle, které blokuje tyto operace.

Operace se záznamy registru

- **Úprava nastavení spuštění** – všechny změny v nastavení, definující, které aplikace budou spouštěny při startu operačního systému Windows. Zobrazíte je například vyhledáním klíče Run v Editoru registru Windows.
- **Vymazání z registru** – vymazání klíče nebo hodnoty.
- **Přejmenování klíče registru** – přejmenování konkrétního klíče.
- **Úprava registru** – vytvoření nové hodnoty nebo změna existujících hodnot. Přesouvání dat v rámci datové struktury. Nastavení uživatelských nebo skupinových práv pro dané klíče registru.

Při zápisu cíle můžete použít zástupné znaky s jistými omezeními. Místo specifikování klíče můžete použít v cestě k registru * (hvězdičku) ve významu "libovolný jeden klíč". Například `HKEY_USERS*\software` může znamenat `HKEY_USER\default\software`, ale ne `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\default\software`.
i `HKEY_LOCAL_MACHINE\system\ControlSet*` není platná cesta ke klíči registru. Cesta registru ukončená * má speciální význam, znamená "tento klíč nebo libovolný podklíč libovolně hluboko". U souborových cílů se dá používat hvězdička pouze tímto způsobem. U vyhodnocování platí, že vždy se hledá nejprve cíl, který popisuje danou cestu přesně, a až poté cíl, který ji popisuje zástupným znakem (*).

! 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. Přepínačem aktivujte možnost **Upozornit uživatele** pro zobrazení oznámení 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 zablokuje jakýkoli pokus definovaných aplikací o zápis do libovolného souboru.
9. Vytvoření nového pravidla potvrdíte kliknutím na tlačítko **OK**.

Nastavení pravidla HIPS ?

Název pravidla

Bez názvu

Akce

Povolit

Operace ovlivní

Cílové soubory



Aplikace



Záznamy registru



Zapnuto



Zaznamenávat od úrovně

Žádná

Upozornit uživatele



Zpět

Další

Zrušit

Přidat cestu k aplikaci/registru pro HIPS

Kliknutím na ... vyberte cestu k aplikaci. Pokud vyberete složku, všechny aplikace v této složce budou zahrnuty do daného pravidla.

Kliknutím na **Otevřít Editor registru** spustíte Editor registru Windows (regedit). Během přidávání zadejte správnou cestu do pole **Hodnota**.

Příklad cesty k souboru nebo v registru:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Aktualizace

Možnosti nastavení aktualizace jsou k dispozici v [Rozšířených nastaveních](#) > **Aktualizace**. Tato sekce vám poskytne informace o aktualizacích serverech a datech pro tyto servery.

Aktualizace

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

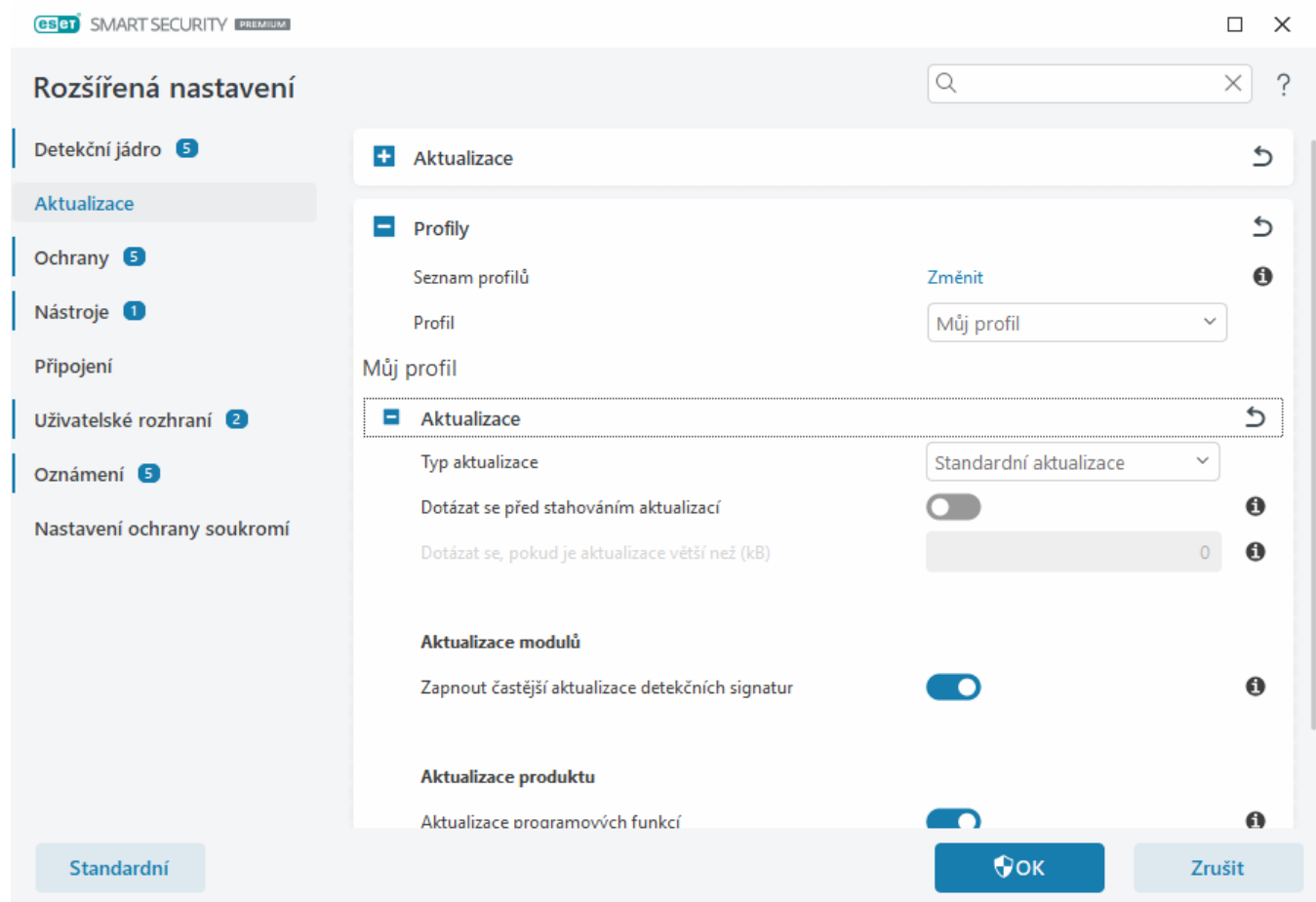
Pro vytvoření nového profilu přejděte do kapitoly [Profily aktualizace](#).

Automatické přepnutí profilu – umožňuje přiřadit profil aktualizace ke konkrétnímu [profilu síťového připojení](#).

Pokud se při pokusu o stažení aktualizací detekčního jádra nebo modulu vyskytnou potíže, klikněte na **Vyčistit** vedle položky **Vyprázdnit aktualizací cache** a vymažte dočasné soubory aktualizací.

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.



Pro správné fungování aktualizace je nezbytné zadat veškeré aktualizací informace správně. Pokud používáte firewall, ujistěte se, že program ESET má povolenou komunikaci s internetem (například komunikaci HTTP).

Profily

Aktuální profily můžete použít pro různá nastavení aktualizací. Vytvoření aktualizací 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 **Aktuální 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.

Dotázat se před stahováním aktualizací – zapne zobrazování oznámení, ve kterém lze zvolit, zda aktualizaci chcete přijmout nebo odmítnout.

Dotázat se, pokud je aktualizace větší než (kB) – program zobrazí potvrzovací dialog, pokud je velikost souboru aktualizace větší než zadaná hodnota. Pokud je velikost aktualizacího souboru nastavena na 0 kB, program zobrazí potvrzovací dialog vždy.

Aktualizace modulů

Zapnout častější aktualizace detekčních signatur – zapnutím této možnosti se budou detekční signatury aktualizovat v kratších intervalech. Deaktivace tohoto nastavení může mít negativní dopad na rychlost detekce.

Aktualizace produktu

Aktualizace programových funkcí – automaticky instaluje nové verze ESET Smart Security Premium.

Možnosti připojení

Jak používat proxy server ke stahování aktualizací si prostudujte v kapitole [Možnosti připojení](#).

Obnovení předchozí verze modulů

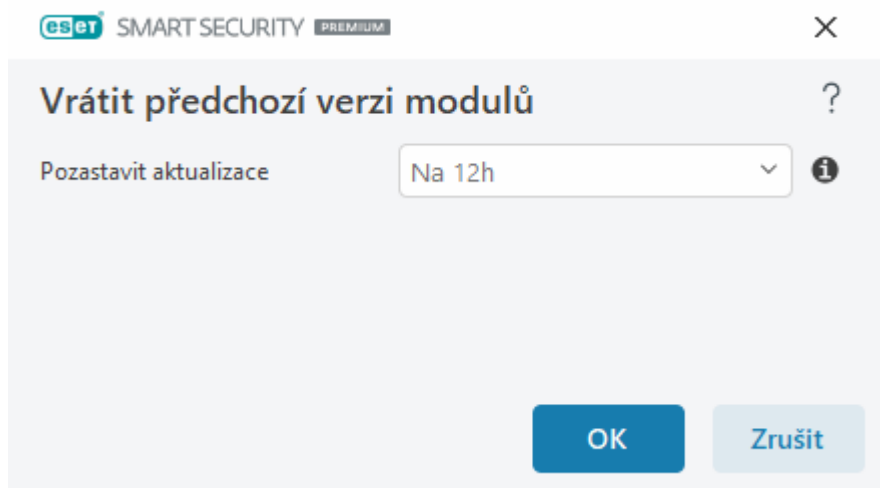
Pokud máte podezření, že nová verze detekčního jádra je nestabilní nebo poškozená, můžete se vrátit ke starší verzi a na stanovený časový interval zakázat jejich aktualizaci. Případně můžete povolit dříve zakázané aktualizace, pokud jste je odložili na neomezeně dlouhou dobu.

ESET Smart Security Premium 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.



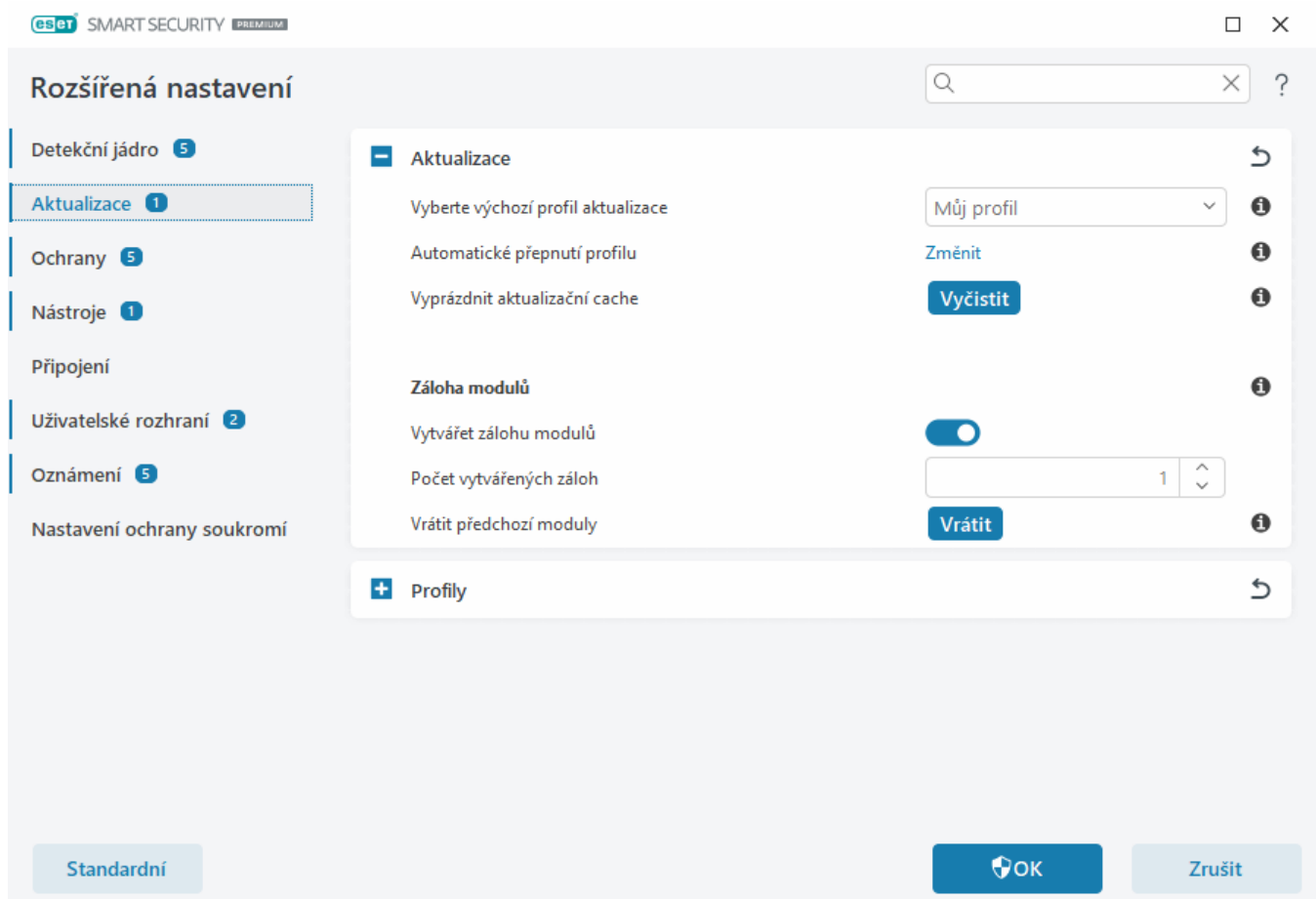
Při dosažení maximálního počtu vytvářených záloh (například tří), dojde každých 48 hodin k nahrazení nejstarší zálohy novou. ESET Smart Security Premium se při obnovení předchozí verze detekčního jádra a programových modulů vrátí vždy k nejstarší verzi.

Pokud kliknete na tlačítko **Vrátit v Rozšířených nastaveních** > **Aktualizace** > **Aktualizace** 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.

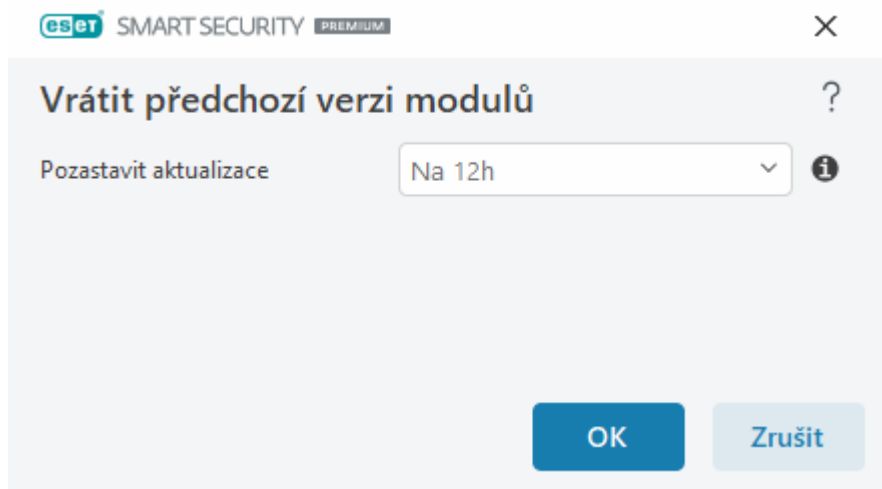
Po obnovení předchozí verze modulů se tlačítko **Vrátit** změní, a bude sloužit pro akci **Povolit aktualizace**. Aktualizace se přeruší na dobu definovanou v dialogovém okně **Pozastavit aktualizace na**. Ze zálohy se obnoví nejstarší verze detekčního jádra a programových modulů uložená v souborovém systému počítače.



Nejnovější verze detekčního jádra má číslo 22700. Na pevném disku počítače jsou uloženy obrazy detekčního jádra 22698 a 22696. Všimněte si, že verze 22697 není k dispozici. Počítač byl totiž delší dobu vypnutý, proto byla stažena novější verze modulů. Pokud jste jako **Počet vytvářených záloh** nastavili číslo 2, po **navrácení změn** se obnoví detekční jádro (i programové moduly) s číslem 22696. Tento proces může chvíli trvat. Pro ověření, zda došlo k obnovení starší verze přejděte v hlavním okně programu na záložku [Aktualizace](#).

Interval pro obnovení předchozí verze modulů

Pokud kliknete na tlačítko **Vrátit** v [Rozšířených nastaveních](#) > **Aktualizace** > **Aktualizace** 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.

Aktualizace produktu

V části **Aktualizace produktu** můžete povolit automatickou instalaci nových funkcí produktu ve chvíli, kdy jsou dostupné.

Aktualizace programových funkcí přináší nové funkce, nebo upravují již existující z předchozích verzí. Aktualizace může probíhat automaticky bez interakce uživatele, nebo po jejím odsouhlasení. Po instalaci aktualizace programové funkce může být zapotřebí restart počítače.

Aktualizace programových funkcí – pokud je tato možnost aktivní, bude docházet k automatické aktualizaci funkcí produktu.

Možnosti připojení

Chcete-li získat přístup k možnostem nastavení proxy serveru pro konkrétní profil aktualizace, otevřete [Rozšířená nastavení](#) > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení**. 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 [Rozšířených nastaveních](#) > **Připojení** > **Proxy server**.

Pomocí možnosti **Nepoužívat proxy server** zajistíte, aby se při aktualizaci ESET Smart Security Premium nepoužíval proxy server.

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

- Pro aktualizaci ESET Smart Security Premium se používá jiný proxy server než ten, který je definován v [Rozšířených nastaveních](#) > **Připojení**. Při takové konfiguraci definujete 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 Smart Security Premium se připojí k proxy serveru z důvodu aktualizace.
- Počítač je připojen k internetu pomocí proxy serveru. Nastavení jsou převzata z Internet Exploreru během instalace programu, pokud se však změní (například při změně poskytovatele internetu), ujistěte se, že nastavení proxy serveru uvedené v tomto okně je správné. 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 aktualizacím serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.

i **Uživatelské jméno a Heslo** v této části jsou pro proxy server specifické. Tato pole vyplňte pouze v případě, kdy jsou vyžadovány údaje pro přístup k proxy serveru. Stává se tak v situaci, kdy pro přístup k internetu prostřednictvím proxy serveru je nutné zadat heslo.

Ochrany

Ochrany chrání systém před útoky škodlivého kódu tím, že kontroluje komunikaci se soubory, e-maily a internetem. Například pokud je detekován objekt klasifikovaný jako malware, zahájí se akce pro vyřešení situace. Škodlivý kód může být zablokován a následně léčen, odstraněn nebo přesunut do karantény.

Chcete-li podrobně nakonfigurovat ochrany, otevřete [Rozšířená nastavení](#) > **Ochrany**.

! Změny v Ochránách by měl provádět pouze zkušený uživatel. Chybnou úpravou nastavení se může snížit úroveň ochrany.

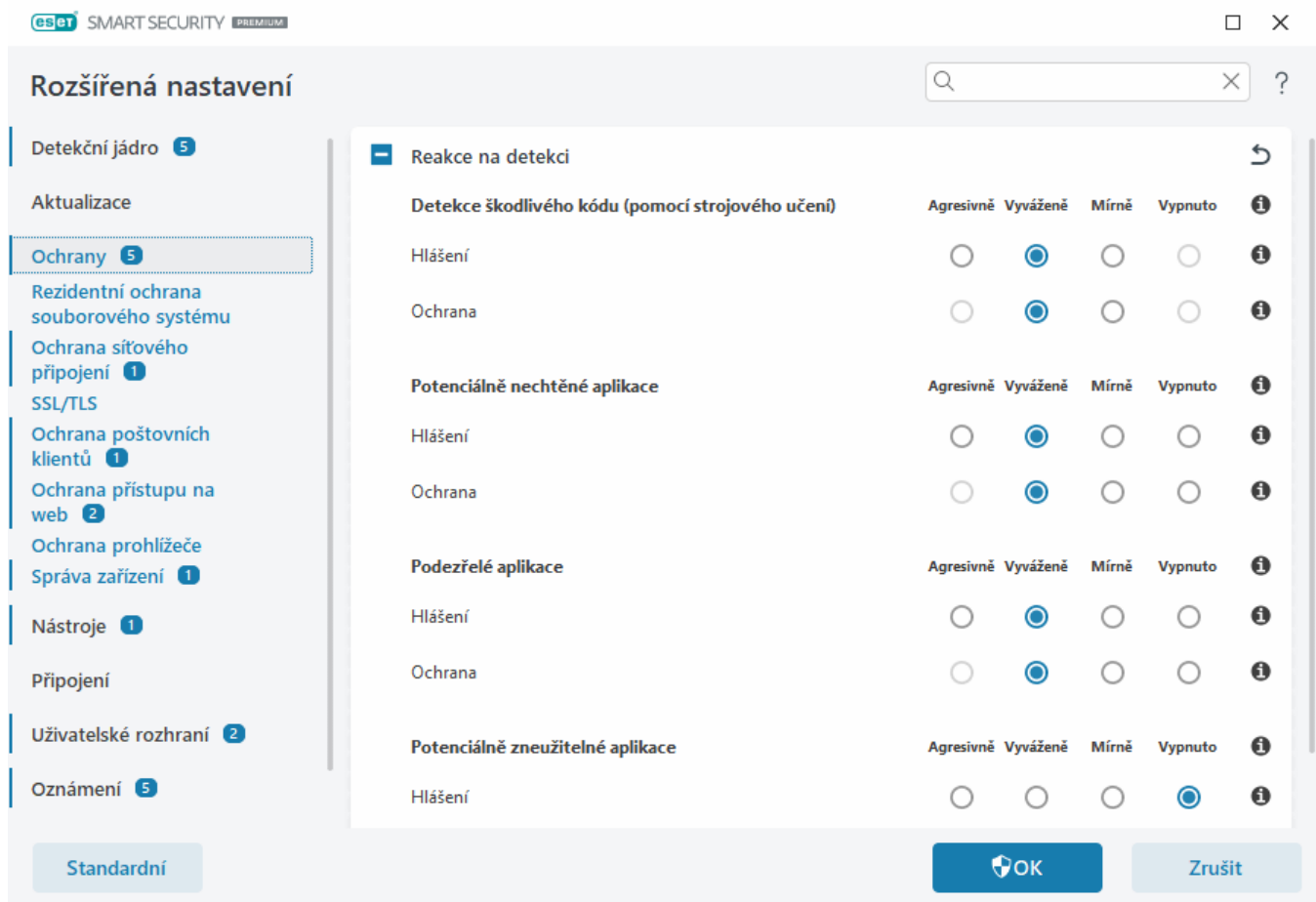
V této kapitole naleznete:

- [Reakce na detekci](#)
- [Nastavení hlášení](#)
- [Nastavení ochrany](#)

Reakce na detekci

Reakce na detekci umožňují nastavit úroveň hlášení a ochrany pro následující kategorie:

- **Detekce škodlivého kódu (pomocí strojového učení)** – počítačový virus je část škodlivého kódu, která je připojena k existujícím souborům v počítači. Termín "virus" bývá často vykládán nesprávně. Vhodnějším výrazem je "malware" (škodlivý software). Detekce malwaru zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).
- **Potenciálně nechtěné aplikace** – grayware (neboli PUA – potentially unwanted application) představují širokou škálu aplikací, které nejsou jednoznačně škodlivé jako viry nebo trojské koně. Mohou však instalovat nechtěný software, měnit chování vašeho zařízení, provádět neočekávané operace, případně akce bez vědomí uživatele. Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).
- Mezi **potenciálně podezřelé aplikace** řadíme rovněž programy, které jsou komprimovány pomocí [packerů](#) nebo protektorů. Tuto metodu často využívají tvůrci škodlivého kódu, aby se vyhnuli detekci ze strany antiviru.
- **Potenciálně zneužitelné aplikace** – legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti. Příkladem mohou být programy pro vzdálené připojení, aplikace k odšifrování hesel a keyloggery (programy, které zaznamenávají uživatelem zadané znaky na klávesnici). Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).



Vylepšená ochrana

- i** Pokročilé strojové učení je nyní funguje jako pokročilá vrstva ochrany a vylepšuje tak detekci. Pro více informací o tomto typu ochranu se podívejte do [slovníku pojmů](#).

Nastavení hlášení

Při výskytu detekce (například při objevení hrozby klasifikované jako malware) se informace zapíše do [Detekčního protokolu](#) a může se zobrazit [Oznámení na pracovní ploše](#) (pokud je to v produktu ESET Smart Security Premium povoleno).

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

1. Detekce škodlivého kódu
2. Potenciálně nechtěné aplikace
3. Potenciálně zneužitelné aplikace
4. Podezřelé aplikace

Hlášení zajišťuje detekční jádro včetně komponenty strojového učení. Pro hlášení můžete nastavit vyšší práh, než je aktuální úroveň [ochrany](#). Tato nastavení nemají vliv na blokování, [léčení](#) nebo odstraňování [objektů](#).

Před změnou prahu (úrovně) pro danou KATEGORII si přečtěte níže uvedené informace:

Práh	Vysvětlení
Agresivně	Hlášení z dané KATEGORIE je nakonfigurováno na nejvyšší citlivost. Hlášeno bude větší množství detekcí. V agresivním nastavení může docházet k chybné identifikaci některých objektů patřících do KATEGORIE.
Vyváženě	Hlášení z dané KATEGORIE je nakonfigurováno jako vyvážené. Toto nastavení je optimalizováno s ohledem na výkon, přesnost detekce a množství falešných poplachů.
Mírně	Hlášení z dané KATEGORIE je nakonfigurováno tak, aby se minimalizoval počet falešných poplachů při zachování dostatečné úrovně zabezpečení. Objekty budou hlášeny pouze v případě vysoké pravděpodobnosti a shody chování odpovídající KATEGORII.
Vypnuto	Hlášení pro danou KATEGORII není aktivní a detekce tohoto typu nebudou zachytávány, hlášeny ani léčeny. V důsledku tohoto nastavení bude vypnuta ochrana před tímto typem detekce. V rámci hlášení malware není k dispozici možnost Vypnuto. Tato hodnota je výchozí pro potenciálně zneužitelné aplikace.

✓ [Dostupnost modulů ochrany produktu ESET Smart Security Premium](#)

Níže uvádíme dostupnost jednotlivých prahů KATEGORIÍ (zapnuto nebo vypnuto) v modulech ochrany:

	Agresivně	Vyváženě	Mírně	Vypnuto*
Modul pokročilého strojového učení	✓ (agresivní režim)	✓ (konzervativní režim)	X	X
Modul detekčního jádra	✓	✓	✓	X
Ostatní moduly ochrany	✓	✓	✓	X

** Nedoporučeno.

✓ [Jak zjistím verzi produktu, programových modulů a data sestavení?](#)

1. V hlavním okně programu klikněte na **Nápověda a podpora > O programu ESET Smart Security Premium**.
2. V zobrazeném dialogovém okně **O programu** se na prvním řádku zobrazuje číslo verze vámi používaného produktu ESET.
3. Pro zobrazení informací o jednotlivých modulech klikněte na tlačítko **Nainstalované programové komponenty**.

Důležité poznámky

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

- Možnost **Vyváženě** je doporučena pro většinu situací.
- 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 Smart Security Premium a jeho moduly aktuální](#).

Nastavení ochrany

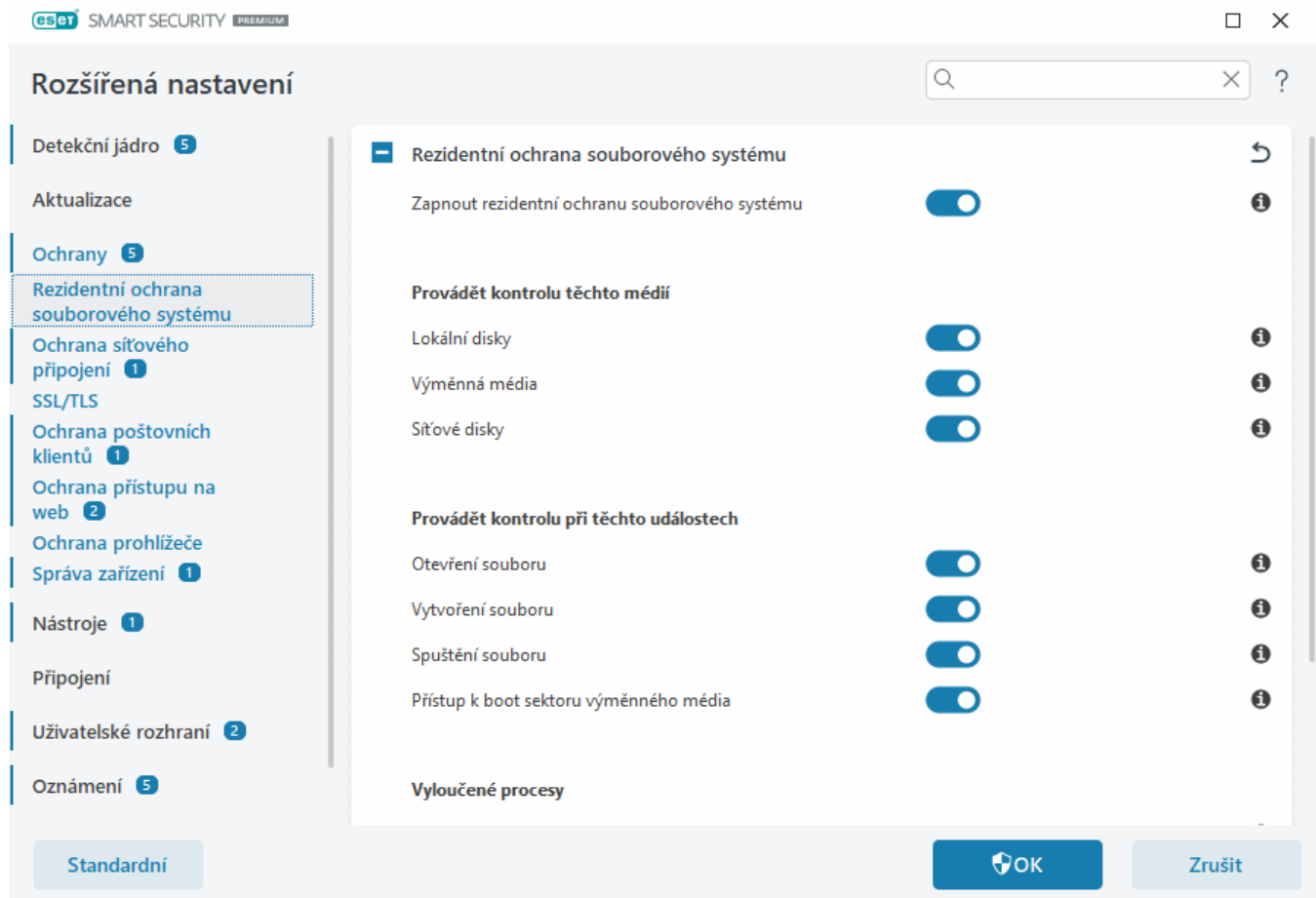
Pokud je detekovaný objekt klasifikován jako KATEGORIE, program jej zablokuje, a následně [vyléčí](#), odstraní nebo přesune do [karantény](#).

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.

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 [Rozšířených nastaveních](#) > **Ochrany** > **Rezidentní ochrana souborového systému** > **Rezidentní ochrana souborového systému**.

Kontrola médií

Standardně je nastavena kontrola všech typů médií:

- **Lokální disky** – kontroluje všechny systémové a lokální pevné disky (například `C:\`, `D:\`).
- **Výměnná média** – kontroluje CD, DVD, USB úložiště, paměťové karty, atp.
- **Síťové disky** – kontroluje všechny namapované síťové jednotky (například kdy pod písmenem `H:` máte `\\store04`), stejně tak síťová umístění přímo (například `\\store08`).

Doporučujeme ponechat toto nastavení. Změnu doporučujeme pouze ve zvláštních případech, např. pokud při kontrole určitého média dochází k výraznému zpomalení.

Kontrola při událostech

Standardně jsou kontrolovány všechny soubory, jakmile jsou otevřené, vytvořené nebo spuštěné. Tato nastavení doporučujeme ponechat pro zajištění maximální možné ochrany počítače:

- **Otevření souboru** – zapne/vypne kontrolu otevíraných souborů.
- **Vytvoření souboru** – zapne/vypne kontrolu vytvářených nebo modifikovaných souborů.

- **Spuštění souboru** – zapne/vypne kontrolu spouštěných souborů.
- **Přístup na boot sektor výměnného zařízení** – pokud obsahuje vložené výměnné médium boot sektor, po připojení média do zařízení dojde automaticky ke kontrole sektoru. Tato možnost nezapíná kontrolu souborů na výměnných médiích. Nastavení kontroly na výměnných médiích se nachází v části **Provádět kontrolu těchto médií > Výměnná média**. Aby kontrola boot sektoru výměnných médií fungovala správně, ponechte v ThreatSense zapnutou funkci **Boot sektory/UEFI**.

Vyloučené procesy

Viz [Vyloučené procesy](#).

ThreatSense

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí jako je přístup k souboru. Při kontrole jsou používány detekční metody technologie **ThreatSense** (ty jsou popsány v kapitole [Nastavení skenovacího jádra ThreatSense](#)). Chování rezidentní ochrany souborového systému lze nakonfigurovat tak, aby se s nově vytvořenými soubory zacházelo jinak než s existujícími soubory. Například, pro nově vytvářené soubory můžete nastavit hlubší úroveň kontroly.

Pro zajištění minimálních systémových nároků, nejsou již dříve kontrolované soubory znovu kontrolovány (pokud nebyly změněny). Soubory jsou opět kontrolovány pouze po každé aktualizaci detekčních modulů. Toto chování můžete přizpůsobit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje. Chcete-li toto nastavení upravit, otevřete [Rozšířená nastavení > Ochrany > Rezidentní ochrana souborového systému](#). Klikněte na **ThreatSense > Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

Rezidentní ochrana souborového systému také umožňuje konfigurovat [Další parametry ThreatSense](#).

Vyloučené procesy

Pomocí této funkce vyloučíte z Rezidentní ochrany souborového systému činnost konkrétních procesů. V případě obnovy dedikovaných serverů (aplikačních, souborových atd.) ze zálohy do funkčního stavu hraje kritickou roli čas. Při navýšení rychlosti zálohování, zajištění integrity dat a dostupnosti služeb jsou některá zálohovací řešení technicky v konfliktu s antivirovou ochranou souborového systému. Jediným řešením pro zabránění konfliktu bývá deaktivace anti-malware řešení. Vyloučením činnosti konkrétních procesů (například zálohovacího agenta) z kontroly je veškerá jejich činnost ignorována a považována za důvěryhodnou, čímž je minimalizován vliv na celý průběh operace (například zálohování). Při vytváření výjimek však buďte obezřetní. Při přístupu zálohovacího agenta k infikovanému souboru nedojde k detekci a hlášení hrozby. Z tohoto důvodu je možné výjimky vytvářet pouze z rezidentní ochrany souborového systému.



Nezaměňujte tuto funkci s možností pro [vyloučení přípon souborů](#) z kontroly, tvorbu [HIPS výjimek](#), [detekčních výjimek](#) nebo [výkonnostních výjimek](#).

Prostřednictvím těchto výjimek můžete minimalizovat možné konflikty a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (.exe).

Spustitelné soubory můžete přidat do seznamu vyloučených procesů v [Rozšířených nastaveních > Ochrany > Rezidentní ochrana souborového systému > Rezidentní ochrana souborového systému > Vyloučené procesy](#).

Tato funkce byla navržena pro vytvoření výjimek na zálohovací nástroje. Vyloučením zálohovacích nástrojů z kontroly nemá pouze vliv na stabilitu systému, ale také rychlost zálohování.

- ✓ Kliknutím na **Změnit** si otevřete správce **Výjimek**, kde pomocí tlačítka **Přidat** a použitím průzkumníka vyberete spustitelný soubor (například *Backup-tool.exe*), který chcete vyloučit z kontroly. Po přidání .exe souboru na seznam výjimek přestane ESET Smart Security Premium 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**.

- i 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 Smart Security Premium monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

- ! Pokud pro výběr procesu nevyužijete průzkumníka, zadejte absolutní cestu k procesu manuálně. V opačném případě nebude výjimka fungovat korektně a **HIPS** může generovat chyby.

Seznam procesů vyloučených z kontroly můžete kdykoli **upravit**, stejně tak proces ze seznamu výjimek **odstranit**.

Kdy měnit nastavení rezidentní ochrany

Rezidentní ochrana je klíčovým modulem zabezpečujícím ochranu počítače. Proto je potřeba být při změnách nastavení obezřetný. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech.

Po instalaci ESET Smart Security Premium jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Chcete-li obnovit výchozí nastavení, klikněte na ➡ vedle položky v **Rozšířených nastaveních** > **Ochrany** > **Reakce na detekci**.

Ověření funkčnosti rezidentní ochrany

Pro ověření, zda je rezidentní ochrana funkční a detekuje malware, je možné použít bezpečný testovací soubor z webových stránek *www.eicar.com*. Jedná se o soubor, který je detekován všemi antivirovými programy. Byl

vytvořen společností EICAR (European Institute for Computer Antivirus Research) pro testování funkčnosti antivirových programů.

Soubor eicar je dostupný na adrese <http://www.eicar.org/download/eicar.com>.

Po zadání této URL adresy do prohlížeče by se měla objevit zpráva, že hrozba byla odstraněna.

Co dělat, když nefunguje rezidentní ochrana

V této části popisujeme problémové stavy, které mohou nastat při běhu rezidentní ochrany. Je zde také uvedeno jak postupovat při jejich řešení.

Rezidentní ochrana je vypnutá

Pokud uživatel nechtěně zakáže rezidentní ochranu, měli byste funkci znovu aktivovat. 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**. Chcete-li se ujistit, že je tato možnost povolena, otevřete [Rozšířená nastavení](#) > **Ochrany > Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

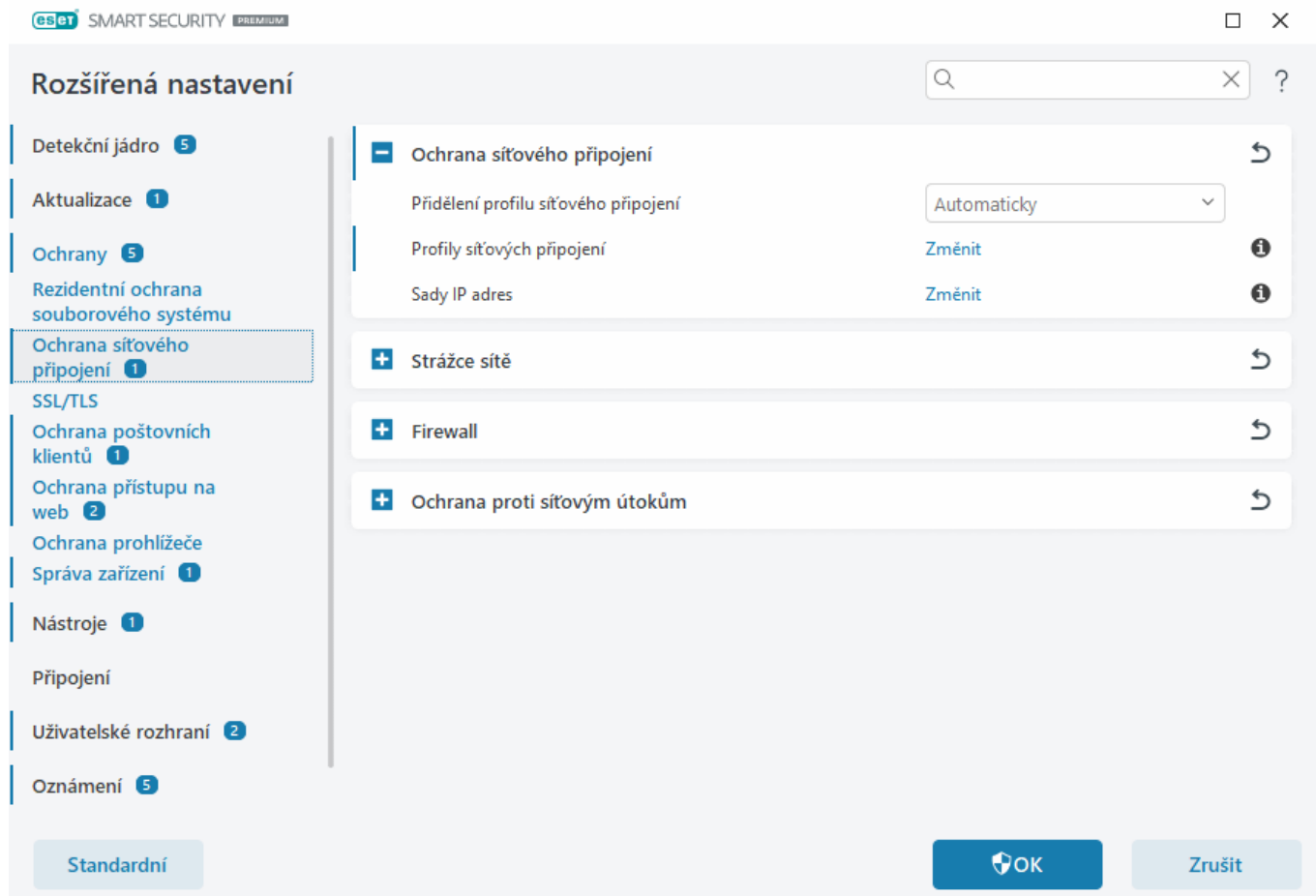
Ujistěte se, zda nemáte nainstalovaný další bezpečnostní program. Pokud jsou na zařízení nainstalované dva bezpečnostní programy, může mezi nimi docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Zapnout rezidentní ochranu souborového systému**, zřejmě dochází ke konfliktu s jiným programem. Pokud chcete problém vyřešit, [vytvořte ESET SysInspector protokol a odešlete jej k analýze technické podpory ESET](#).

Ochrana síťového připojení

Ochrana síťového připojení umožňuje podrobně konfigurovat všechna síťová připojení. Na základě konfigurace můžete povolit/zakázat přístup k počítači v určitých sítích, povolit/zakázat přístup k síťovým zařízením z počítače a další. Ve výchozím nastavení má ESET Smart Security Premium pravidla firewallu a ochranu síťového připojení předem nakonfigurované pro maximální zabezpečení. Ve specifických prostředích však může být nutná vlastní konfigurace. Změnu výchozího nastavení by měl provádět pouze zkušený uživatel.



Následující nastavení můžete nakonfigurovat v části [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** (podrobný popis jednotlivých možností ochrany síťového připojení naleznete po kliknutí na níže uvedené odkazy):

Ochrana síťového připojení

[Profily síťových připojení](#) – pomocí profilů můžete řídit chování firewallu pro konkrétní síťová připojení.

[Sady IP adres](#) – můžete definovat sady IP adres, které vytvářejí jednu logickou skupinu IP adres, kterou lze použít pro [pravidla firewallu](#).

[Strážce sítě](#)

[Firewall](#)

[Ochrana proti síťovým útokům](#)


Profily síťových připojení

Profily lze použít k řízení chování síťové ochrany ESET Smart Security Premium pro konkrétní [síťová připojení](#). Při vytváření nebo úpravě [pravidla firewallu](#), [IDS pravidla](#) nebo [pravidla Ochrany před útoky hrubou silou](#) můžete dané pravidlo přiřadit ke konkrétnímu profilu nebo jej použít pro všechny profily. Pokud je profil v síťovém připojení aktivní, jsou na něj aplikována pouze globální pravidla (pravidla bez zadaného profilu) a pravidla, která byla tomuto profilu přiřazena. Můžete vytvořit více profilů s různými pravidly přiřazenými síťovým připojením a snadno tak změnit chování firewallu.

Profily a přiřazení síťových připojení můžete konfigurovat v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana**

síťového připojení > Ochrana síťového připojení.

Přidělení profilu síťového připojení – umožňuje zvolit, zda má být nově zjištěným síťovým připojením automaticky (v rozbalovacím menu vyberte možnost **Auto**) přiřazen předdefinovaný nebo vlastní profil na základě [Spouštěčů](#) nakonfigurovaných v profilech síťových připojení, nebo zda chcete být při zjištění nového síťového připojení vyzváni (v rozevírací nabídce vyberte možnost **Dotázat se**) ke [konfiguraci ochrany sítě](#) a přiřazení profilu ručně.

Konkrétní profil síťového připojení můžete přiřadit také ručně v [hlavním okně programu](#) > **Nastavení** > **Síťová ochrana** > **Síťová připojení**. Najedťte na konkrétní síťové připojení a kliknutím na ikonu nabídky  > **Změnit** otevřete okno [Nastavení ochrany sítě](#) a vyberte profil.

Profily síťového připojení – kliknutím na **Změnit** [přidáte nebo upravíte profily síťového připojení](#).

Následující profily jsou předdefinované a nelze je upravovat nebo odstraňovat:

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

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

Po přepnutí síťového připojení na jiný profil se v pravém dolním rohu obrazovky zobrazí oznámení.

Přidání nebo úprava profilů síťového připojení

[Profily síťového připojení](#) můžete přidat nebo upravit v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana síťového připojení** > **Ochrana síťového připojení** > **Profily síťových připojení** > **Změnit**. Chcete-li profil upravit, musíte jej vybrat ze seznamu **Profilů síťových připojení**.

Následující profily jsou předdefinované a nelze je upravovat nebo odstraňovat:

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

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

Tlačítka **Nahoru/Výše/Níže/Dolů**     – umožňují nastavit úroveň priority profilů síťového

připojení (profily síťového připojení jsou vyhodnoceny a použity podle své priority. Vždy se použije první odpovídající profil).

Přidání nebo úprava profilu

Vlastní profil síťového připojení umožňuje použít pravidla firewallu a definovat další nastavení pro konkrétní síťová připojení. V sekci [Spouštěče](#) určíte, ke kterým síťovým připojením bude vlastní profil přiřazen.

Chcete-li otevřít editor profilů v okně **Profily síťových připojení**:

- Klikněte na **Přidat**.
- Vyberte jeden z existujících profilů a klikněte na tlačítko **Změnit**.
- Vyberte jeden z existujících profilů a klikněte na tlačítko **Kopírovat**.

Název – název vlastního profilu.

Popis – popis profilu, který pomáhá profil identifikovat.

Vždy důvěryhodné adresy – zde definované adresy jsou přidány do důvěryhodné zóny síťového připojení, na které je tento profil aplikován (bez ohledu na typ ochrany sítě).

Důvěryhodné připojení - vaše zařízení a sdílené soubory uložené ve vašem zařízení jsou viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti (přístup ke sdíleným souborům a tiskárnám je povolen, příchozí soubory a tiskárny jsou dostupné, RPC komunikace je povolena a je k dispozici sdílení vzdálené plochy). Toto nastavení doporučujeme použít při vytváření profilu pro zabezpečené připojení k místní síti. Všechny přímo připojené podsítě jsou rovněž považovány za důvěryhodné. Například, pokud je síťový adaptér připojen k síti s IP adresou 192.168.1.5 a maskou 255.255.255.0, podsít 192.168.1.0/24 bude přidána do důvěryhodné zóny. Pokud má adaptér více adres/podsítí, budou důvěryhodné všechny.

Upozornit na slabě zabezpečenou Wi-Fi síť – po aktivování této možnosti ESET Smart Security Premium zobrazí na ploše [oznámení](#), jestliže se připojíte k nezabezpečené nebo slabě zabezpečené bezdrátové síti.

Spouštěče – vlastní podmínky, které musí být splněny, aby bylo možné přiřadit tento profil síťového připojení k určitému síťovému připojení. Podrobné vysvětlení naleznete v kapitole [Spouštěče](#).

Spouštěče

Spouštěče jsou vlastní podmínky, které musí být splněny, aby bylo možné přiřadit [Profil síťového připojení](#) k [Síťovému připojení](#). Pokud má připojená síť stejné atributy, jaké jsou definovány ve spouštěčích pro profil připojené sítě, bude profil na síť použit. Profil síťového připojení může mít jeden nebo více spouštěčů. Pokud existuje více spouštěčů, platí logika NEBO (musí být splněna alespoň jedna podmínka). Spouštěče můžete definovat v [editoru profilu síťového připojení](#). Vytváření vlastních profilů síťového připojení by měl provádět zkušený uživatel.

K dispozici jsou následující spouštěče (pokud chcete znát podrobnosti o své aktuální síti, podívejte se do kapitoly [Síťová připojení](#)):

✓ [Adaptér](#)

Typ adaptéru – profil se použije, pokud je síťové připojení navázáno pomocí vybraného typu adaptéru.
Název adaptéru – profil se použije, pokud odpovídá názvu síťového adaptéru.
IP adresa adaptéru – profil se použije, pokud odpovídá IP adrese síťového adaptéru.

✓ [DNS](#)

Přípona DNS – profil se použije, pokud mu odpovídá název domény.
IP adresa DNS – profil se použije, pokud mu odpovídá IP adresa DNS serveru.

✓ [WINS](#)

Profil se použije, pokud mu odpovídá IP adresa ve službě Windows Internet Name Service (WINS).

✓ [DHCP](#)

DHCP IP – odpovídá IP adrese serveru DHCP.

✓ [Výchozí brána](#)

IP – profil se použije, pokud mu odpovídá IP adrese výchozí brány.
MAC adresa – profil se použije, pokud se shoduje s MAC adresou výchozí brány.

✓ [Wi-Fi](#)

SSID – profil se použije, pokud mu odpovídá SSID (název Wi-Fi).
Název profilu – profil se použije, pokud mu odpovídá název profilu Wi-Fi.
Typ zabezpečení – profil se použije, pokud typ zabezpečení odpovídá typu vybranému z rozbalovacího menu. Pokud chcete, aby odpovídal více než jeden typ, vytvořte další spouštěč.
Typ šifrování – profil se použije, pokud typ šifrování odpovídá typu vybranému z rozbalovacího menu. Pokud chcete, aby odpovídal více než jeden typ, vytvořte další spouštěč.
Zabezpečení sítě – profil se použije, pokud je síť **otevřená/zabezpečená**.

✓ [Profil systému Windows](#)

Profil se použije, pokud je síť v systému Windows nakonfigurována jako **Doména/Privátní/Veřejná**.

✓ [Ověření](#)

Autentifikace zóny vyhledává v síti specifický server a pro vlastní autentifikaci vůči serveru používá asymetrické šifrování (RSA). Název ověřované sítě musí odpovídat názvu v nastavení ověřovacího serveru. Mějte na paměti, že se v názvu rozlišuje velikost písmen. Název serveru lze zadat jako IP adresu, DNS nebo název NetBios.

[Stáhnout ESET Authentication Server](#)

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

- Veřejný klíč zašifrovaný ve formátu PEM (.pem); tento klíč můžete vygenerovat pomocí ověřovacího serveru ESET
- Šifrovaný veřejný klíč
- Certifikát s veřejným klíčem (.crt)

Pro ověření nastavení klikněte na tlačítko **Otestovat**. Pokud je ověření úspěšné, zobrazí se zpráva Autentifikace k serveru byla úspěšná. Pokud není ověřování správně nakonfigurováno, zobrazí se jedna z následujících chybových zpráv:

Autentifikace k serveru nebyla úspěšná. Neplatný nebo neodpovídající podpis.

Podpis serveru neodpovídá zadanému veřejnému klíči.

Autentifikace k serveru nebyla úspěšná. Název sítě neodpovídá.

Nakonfigurovaný název sítě neodpovídá názvu sítě ověřovacího serveru. Je nutné, aby zóny byly pojmenovány stejně.

Autentifikace k serveru nebyla úspěšná. Neplatná nebo žádná odpověď od serveru.

Žádná odpověď, server neběží nebo není dostupný. Neplatnou odpověď můžete obdržet, pokud na dané adrese běží jiný HTTP server.

Zadaný veřejný klíč je neplatný.

Ověřte, že je veřejný klíč zadán správně.

Sady IP adres

Sada IP adres je skupina IP adres, které vytvářejí jednu logickou skupinu adres IP, což je užitečné při opakovaném použití stejné sady adres ve více [pravidlech firewallu](#) nebo [pravidlech ochrany proti útokům hrubou silou](#). ESET Smart Security Premium obsahuje také předdefinované sady IP adres, pro které se použijí interní pravidla. Příkladem takové skupiny je **Důvěryhodná zóna**. Důvěryhodná zóna představuje skupinu síťových adres, kde je vaše zařízení a sdílené soubory uložené ve vašem zařízení viditelné pro ostatní uživatele sítě a systémové prostředky jsou přístupné ostatním uživatelům v síti.

Přidání sady IP adres:

1. Otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Sady IP adres** > **Změnit**.

2. Klikněte na tlačítko **Přidat**, zadejte **název** a **popis** zóny, a nakonec zadejte **vzdálenou adresu počítače (definovanou pomocí IPv4/IPv6 adresy, rozsahu, masky)**.

3. Klikněte na tlačítko **OK**.

Další informace naleznete v kapitole [Úprava sad IP adres](#).

Úprava sad IP adres

Další informace o sadách IP adres naleznete v kapitole [Sady IP adres](#).

Sloupce

Název – název skupiny vzdálených počítačů.

Popis – obecný popis skupiny.

IP adresy – vzdálené IP adresy, které patří do sady IP adres.

Ovládací prvky

Při **přidávání** nebo **úpravách** sady IP adres jsou k dispozici následující pole:

Název – název skupiny vzdálených počítačů.

Popis – obecný popis skupiny.

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

Odstranit – odebere zónu ze seznamu.

 Předdefinované sady IP adres nelze odstranit.

Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).

Rozsah adres – umožní zadat počáteční a koncovou IP adresu pro rozsah IP adres několika zařízení (například *192.168.0.1-192.168.0.99*).

✓ **Podsít** – umožní zadat podsít skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsít 192.168.1.0. Chcete-li vyloučit celou podsít, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například

2001:718:1c01:16:214:22ff:fec9:ca5).

Podsít – podsít skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Strážce sítě

[Strážce sítě](#) vám pomůže najít ve vámi označené síti jako důvěryhodné (například domácí nebo firemní síti) zranitelnosti, jako jsou otevřené porty nebo slabé heslo k routeru. Dokáže zobrazit všechna zařízení připojená do vaší domácí sítě a roztřídit je dle typů (např. tiskárny, telefony, herní konzole a další chytrá zařízení aj.). Strážce sítě můžete nakonfigurovat v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana síťového připojení** > **Strážce sítě**.

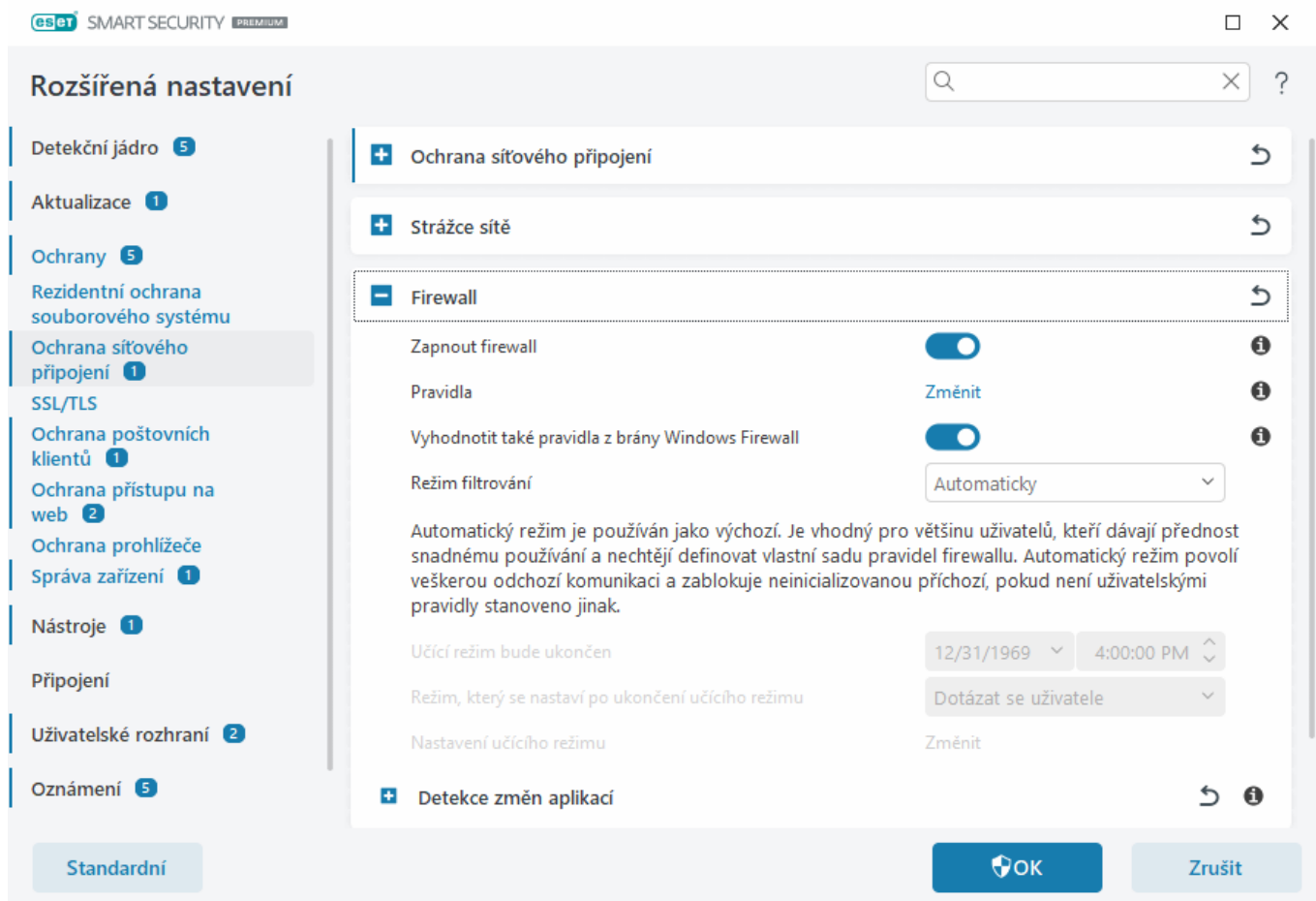
Zapnout Strážce sítě – [Strážce sítě](#) pomáhá identifikovat zranitelná místa v síti, například otevřené porty nebo slabé heslo routeru, a poskytuje seznam připojených zařízení rozdělených do kategorií podle typu zařízení.

Upozornění na nově objevená síťová zařízení – upozorní vás, když je v síti detekováno nové zařízení.

Firewall

Firewall řídí veškerý příchozí a odchozí síťovou komunikaci na vašem zařízení na základě interních a vámi definovaných pravidel. Toho se dosáhne povolením nebo zakázáním jednotlivých síťových připojení. Úkolem firewallu je zablokovat příchozí útoky ze vzdálených zařízení a blokovat nežádoucí služby a aplikace.

Chcete-li nakonfigurovat Firewall, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Firewall**.



Firewall

Zapnout firewall

Pro zajištění bezpečnosti systému doporučujeme ponechat tuto funkci aktivní. Pokud je Firewall povolen, síťová komunikace se kontroluje v obou směrech.

Pravidla

Nastavení pravidel umožňuje [zobrazit a upravit všechna pravidla firewallu](#) aplikovaná na komunikaci mezi aplikacemi v rámci důvěryhodných zón a internetu.



V případě, že na váš počítač útočí [Botnet](#), můžete si vytvořit pravidlo IDS. Pravidlo upravíte v části [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **IDS pravidla**, kliknutím na **Změnit**.

Vyhodnotit také pravidla z brány Windows Firewall

V režimu automatického filtrování také povolí příchozí provoz povolený pravidly z Windows Firewallu, pokud není výslovně blokován pravidly ESET.

Režim filtrování

Chování firewallu záleží na vybraném režimu. Zároveň ovlivňuje míru interakce s uživatelem.

Ve firewallu produktu ESET Smart Security Premium jsou dostupné následující režimy pro filtrování komunikace:

Režim filtrování	Popis
Automatický režim	Přednastavený mód. Je určen pro uživatele, kteří preferují rychlé a pohodlné fungování firewallu bez nutnosti definování pravidel. Vlastní pravidla vytvářet můžete, ale nejsou pro běh Automatického režimu vyžadována. Tento režim povoluje veškerou komunikaci z daného systému směrem ven a blokuje většinu příchozí komunikace kromě komunikace z Důvěryhodné zóny (definované v IDS a rozšířeném nastavení/Povolené služby) odpovídající na nedávnou odchozí komunikaci na stejnou vzdálenou stranu.
Interaktivní režim	Umožňuje nastavení firewallu na míru podle požadavků uživatele. V případě zjištění jakékoli komunikace, na kterou není možné aplikovat žádné existující pravidlo, se uživateli zobrazí dialogové okno s výběrem akce. Následně je možné tuto komunikaci povolit nebo zamítnout, přičemž z tohoto rozhodnutí můžete vytvořit nové pravidlo. V takovém případě bude každá další komunikace tohoto typu v budoucnu povolena nebo zablokována, podle tohoto pravidla. Tento režim však není vhodný pro dlouhodobé používání. Doporučujeme deaktivovat interaktivní režim, jakmile dokončíte vytváření požadovaných pravidel. Při volbě tohoto režimu ve firemním prostředí buďte opatrní, protože nepozorný uživatel může omylem vytvořit pravidla, která by ho mohla vystavit bezpečnostnímu riziku nebo mu znemožnit komunikaci v rámci firemní sítě.
Administrátorský režim	– blokuje každé spojení, pro které neexistuje povolující pravidlo. Tento režim je určen pro pokročilé uživatele, kteří potřebují definovat pravidla pro konkrétní bezpečné spojení. Každá další nespecifikovaná komunikace je firewallem blokována.
Učící režim	Automaticky vytváří pravidla a je vhodný pro prvotní konfiguraci firewallu. Vytvoření pravidel proběhne bez interakce uživatele, protože ESET Smart Security Premium pravidla vytvoří na základě předem definovaných parametrů. Tento režim není bezpečný a doporučujeme jej používat pouze krátkodobě po instalaci, dokud se nevytvoří pravidla pro veškerou nutnou komunikaci.

Učící režim bude ukončen – nastavte datum a čas, kdy se učící režim automaticky ukončí. Učící režim můžete také kdykoli ručně vypnout.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte, ke kterému režimu filtrování se vrátí firewall po ukončení učícího režimu. Další informace o režimech filtrování najdete v tabulce výše. Po dokončení vyžaduje možnost **Dotázat se uživatele** oprávnění administrátora k provedení změny režimu filtrování firewallu.

[Nastavení učícího režimu](#) – kliknutím na tlačítko **Upravit** nakonfigurujete parametry pro ukládání pravidel vytvořených v učícím režimu.

Detekce změn aplikací

Funkce [Detekce změn aplikací](#) zobrazí oznámení v případě, kdy se změněná aplikace, pro kterou existuje pravidlo brány firewall, pokusí navázat komunikaci.

Nastavení učicího režimu





Firewall produktu PRODUCTNAME obsahuje učicí režim, ve kterém je pro každou komunikaci vytvořeno a uloženo odpovídající pravidlo. Není nutná žádná interakce s uživatelem, protože ESET Smart Security Premium ukládá pravidla podle předem definovaných parametrů.

Tento režim není bezpečný a doporučujeme jej používat pouze pro prvotní konfiguraci firewallu.

Chcete-li aktivovat možnosti Učicího režimu, vyberte možnost **Učení** z rozbalovacího menu v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Režim filtrování**. Klikněte na **Upravit** vedle položky **Nastavení učicího režimu** a nakonfigurujte následující možnosti:



V učicím režimu firewall nefiltruje komunikaci. Povolená je veškerá odchozí a příchozí komunikace. Počítač v tomto režimu není plnohodnotně chráněn firewallem.

-  **Příchozí komunikace z důvěryhodné zóny** – vzdálený počítač z důvěryhodné zóny se pokouší komunikovat s lokální aplikací běžící na počítači.
-  **Odchozí komunikace do důvěryhodné zóny** – lokální aplikace se pokouší komunikovat s jiným zařízením v lokální síti nebo s jinou sítí v důvěryhodné zóně.
-  **Příchozí komunikace z internetu** – vzdálený počítač se pokouší komunikovat s aplikací běžící na počítači.
-  **Odchozí komunikace do internetu** – aplikace běžící na počítači se pokouší komunikovat se vzdáleným počítačem.

V každé sekci můžete definovat parametry nově vytvářených pravidel:

Přidat lokální port – číslo lokálního portu síťové komunikace. Pro odchozí spojení se generují náhodná čísla portů. Z tohoto důvodu doporučujeme tuto funkci povolit pouze pro příchozí komunikaci.

Přidat aplikaci – název lokální aplikace. Je doporučeno použít tehdy, pokud chcete do pravidla zahrnout kompletní komunikaci specifikované aplikace. Tedy např. povolit komunikaci pro prohlížeč webových stránek, poštovního klienta apod.

Přidat vzdálený port – číslo vzdáleného portu síťového spojení. Příkladem může být povolení nebo zakázání konkrétní služby se běžným číslem portu, např. HTTP – 80, POP3 – 110 apod.

Přidat vzdálenou IP adresu / důvěryhodnou zónu – vzdálená IP adresa nebo celá zóna adres může být použita jako parametr při vytváření nového pravidla, které se použije na všechny síťové spojení mezi lokálním systémem a těmito adresami. Vhodné použít v případě, pokud chcete definovat akce pro konkrétní zařízení nebo skupinu zařízení v síti.

Maximální počet různých pravidel pro jednu aplikaci – pokud aplikace komunikuje více směry (z různých portů, na různé IP adresy a pod.), poté pro ně firewall v učicím režimu vytvoří odpovídající počet pravidel. Tímto je možné omezit počet pravidel, které mohou být vytvořeny pro jednu aplikaci.

Pravidla firewallu

Pravidla firewallu představují seznam podmínek, podle kterých jsou testována všechna síťová spojení, a jsou k nim přiřazené akce. V části Pravidla firewallu můžete definovat akce pro situace, kdy je navázáno několik síťových spojení.

Pravidla jsou vyhodnocována shora dolů a jejich priorita je uvedena v prvním sloupci. Pro každou komunikaci se provede první vyhovující pravidlo.

Z hlediska směru komunikace je možné provést rozdělení spojení na příchozí a odchozí. Příchozí spojení je iniciováno na vzdálené straně a snaží se navázat spojení s lokální stranou. V případě odchozího spojení je situace opačná, tedy lokální strana navazuje spojení se vzdáleným počítačem.



V případě zjištění neznámé komunikace je potřeba zvážit, zda ji povolit nebo zamítnout. Nevyžádané, nezabezpečené nebo zcela neznámé spojení představuje pro systém bezpečnostní riziko. Při takové komunikaci je vhodné věnovat pozornost především vzdálené straně a aplikaci, která se pokouší navázat toto spojení. Mnoho infiltrací odesílá soukromá data nebo stahuje další škodlivé aplikace na počítač. Právě tato skrytá spojení je možné pomocí firewallu odhalit a zakázat.

Pravidla firewall můžete zobrazit a upravit v části [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Pravidla** > **Změnit**.

Pokud máte mnoho pravidel firewallu, můžete pomocí filtru zobrazit pouze konkrétní pravidla. Chcete-li filtrovat pravidla firewallu, klikněte na možnost **Další filtry** nad seznamem pravidel firewallu. Pravidla můžete filtrovat podle následujících kritérií:

- Původ
- Směr
- Akce
- Dostupnost

Ve výchozím nastavení jsou předdefinovaná pravidla firewallu skrytá. Chcete-li zobrazit všechna předdefinovaná pravidla, deaktivujte přepínačem volbu **Skrýt vestavěná (předdefinovaná) pravidla**. Tato pravidla můžete deaktivovat, ale nemůžete je odstranit.

 Klikněte na ikonu vyhledávání  vpravo nahoře a vyhledejte pravidlo (pravidla).

Sloupce

Priorita – pravidla jsou vyhodnocována shora dolů a jejich priorita je uvedena v prvním sloupci.

Zapnuto - ukazuje, zda je pravidlo aktivní nebo ne; pro aktivaci pravidla musí být zaškrtnuto příslušné políčko.

Aplikace – název aplikace, pro kterou platí pravidlo.

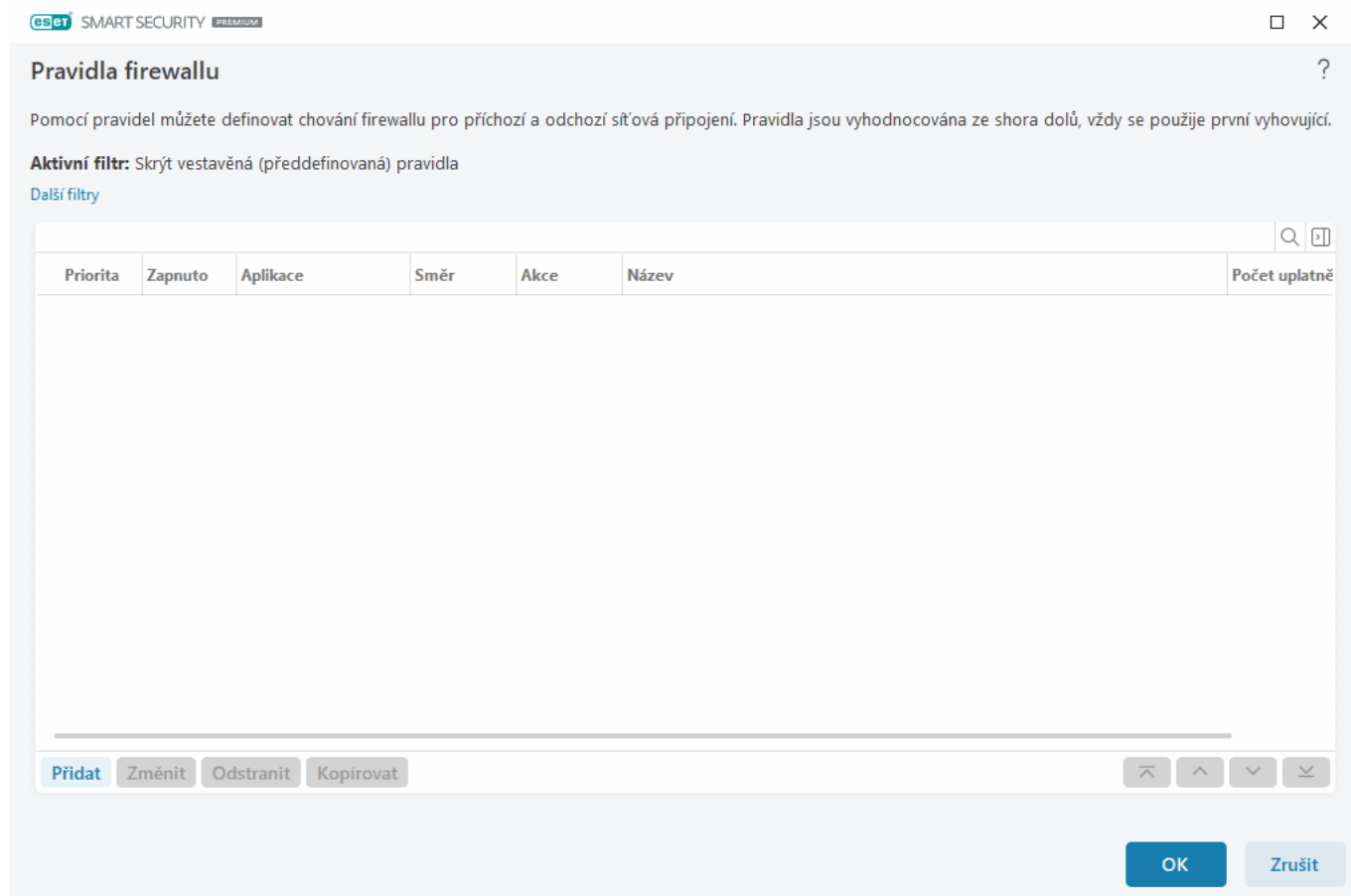
Směr – směr komunikace (příchozí/odchozí/oba).

Akce – akce, která se s komunikací provede (zablokovat/povolit/dotázat se).

Název – název pravidla. Ikona ESET  představuje předdefinované pravidlo.

Počet uplatnění – celkový počet použití pravidla.

Kliknutím na ikonu rozbalení  zobrazíte podrobnosti o pravidle.



Pravidla firewallu

Pomocí pravidel můžete definovat chování firewallu pro příchozí a odchozí síťová připojení. Pravidla jsou vyhodnocována ze shora dolů, vždy se použije první vyhovující.

Aktivní filtr: Skryt vestavěná (předdefinovaná) pravidla

Další filtry

Priorita	Zapnuto	Aplikace	Směr	Akce	Název	Počet uplatně
----------	---------	----------	------	------	-------	---------------

Přidat Změnit Odstranit Kopírovat

OK Zrušit

Ovládací prvky

Přidat – kliknutím [vytvoříte nové pravidlo](#).

Změnit – kliknutím [upravíte existující pravidlo](#).

Odstranit – kliknutím odstraníte existující pravidlo.

Kopírovat – kliknutím vytvoříte kopii existujícího pravidla.



Nahoru/Výše/Dolů/Níže – pomocí těchto tlačítek změníte pořadí vyhodnocování pravidel (vyhodnocována jsou shora dolů).

Přidání a úprava pravidel firewallu

Pravidla firewallu představují podmínky, podle kterých jsou testována všechna síťová připojení, a jsou k nim přiřazené akce. Vytvoření nového nebo změna stávajícího pravidla firewallu je vyžadována vždy, když dojde ke změně sledovaných parametrů spojení. V takovém případě totiž pravidlo již nesplňuje podmínku a není tedy na něj uplatněna definovaná akce. V konečném důsledku to může znamenat zamítnutí spojení a následné problémy s funkcí aplikace. Příkladem je změna síťové adresy vzdálené strany nebo čísla portu. Zkušený uživatel by měl

vytvořit vlastní Pravidla firewallu.

Názorné ukázky

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

- [Otevření nebo uzavření \(povolení nebo zamítnutí\) konkrétního portu ve firewallu](#) (článek nemusí být dostupný ve všech jazycích)
- [Vytvoření firewallového pravidla z protokolu ESET Smart Security Premium](#)

Chcete-li přidat nebo upravit pravidlo firewallu, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Pravidla** > **Změnit**. V okně [Pravidla firewallu](#) klikněte na tlačítko **Přidat** nebo **Změnit**.

Název – zadejte název pravidla.

Povoleno – kliknutím na přepínač se pravidlo aktivuje.

Přidejte akce a podmínky pro pravidlo firewallu:

✓ [Akce](#)

Akce – vyberte, zda chcete **Povolit** nebo **Blokovat** komunikaci, která odpovídá podmínkám definovaným v tomto pravidle, nebo zda se má ESET Smart Security Premium **Dotázat** při každém navázání komunikace. **Zaznamenávat do protokolu** - pokud bude pravidlo použito, bude zaznamenáno do [Protokolů](#). **Zaznamenávat do úrovně** – zvolte [závažnost záznamu protokolu](#) pro toto pravidlo. **Upozornit uživatele** – zobrazí oznámení, pokud je pravidlo aplikováno.

✓ [Aplikace](#)

Zadejte aplikaci, pro kterou bude toto pravidlo použito.

Cesta k aplikaci – klikněte na a přejděte k aplikaci nebo zadejte celou cestu k aplikaci (např C:\Program Files\Firefox\Firefox.exe). Nezadávejte pouze samotný název aplikace.

Digitální podpis aplikace – pravidlo můžete použít na aplikace na základě jejich signatur (jména vystavitele). Z rozbalovacího menu vyberte, zda chcete pravidlo použít na aplikace s **Jakýmkoli platným podpisem** nebo na aplikace **Podepsané určitým vystavitelem**. Pokud vyberete aplikace **Podepsané určitým vystavitelem**, je třeba zadat vystavitele v poli **Jméno vystavitele**.

Aplikace z Microsoft Store – z rozbalovacího menu vyberte aplikaci nainstalovanou z Microsoft Store.

Služba – místo aplikace můžete vybrat systémovou službu. Otevřete rozbalovací menu a vyberte službu.

Použít na potomky procesu – některé aplikace mohou spouštět více procesů, zatímco vy vidíte pouze jedno okno aplikace. Kliknutím na přepínač povolíte pravidlo pro všechny procesy v zadané aplikaci.

✓ [Směr](#)

Vyberte **Směr** komunikace pro toto pravidlo:

- **Oba** – příchozí i odchozí komunikace
- **Dovnitř** – pouze příchozí komunikace
- **Ven** – pouze odchozí komunikace

✓ [IP protokol](#)

Pokud chcete, aby se toto pravidlo vztahovalo pouze na určitý protokol, vyberte z rozbalovacího menu **Protokol**.

✓ [Lokální hostitel](#)

Lokální adresy, rozsah adres nebo podsít, kde se toto pravidlo použije. Pokud není zadána žádná adresa, pravidlo se použije na veškerou komunikaci s lokálními hostiteli. IP adresy, rozsahy adres nebo podsítě můžete přidávat přímo do textového pole **IP adresa** nebo vybírat z existujících [Sad IP adres](#) kliknutím na tlačítko **Změnit** vedle položky **Sady IP adres**.

✓ [Lokální port](#)

Číslo (čísla) lokálního **portu**. Pokud nejsou zadána žádná čísla, pravidlo se použije pro libovolný port. Můžete přidat jeden komunikační port nebo řadu komunikačních portů.

✓ [Vzdálený hostitel](#)

Vzdálená adresa, rozsah adres nebo podsít, kde se toto pravidlo použije. Pokud není zadána žádná adresa, pravidlo se použije na veškerou komunikaci se vzdálenými hostiteli. IP adresy, rozsahy adres nebo podsítě můžete přidávat přímo do textového pole **IP adresa** nebo vybírat z existujících [Sad IP adres](#) kliknutím na tlačítko **Změnit** vedle položky **Sady IP adres**.

✓ [Vzdálený port](#)

Číslo(a) vzdáleného **portu**. Pokud nejsou zadána žádná čísla, pravidlo se použije pro libovolný port. Můžete přidat jeden komunikační port nebo řadu komunikačních portů.

✓ [Profil](#)

Pravidlo firewallu lze použít na konkrétní [profily síťových připojení](#).

Jakýkoli – pravidlo bude použito na jakékoli síťové připojení bez ohledu na použitý profil.

Vybráno – pravidlo bude použito na konkrétní síťové připojení na základě vybraného profilu. Zaškrtněte políčko vedle profilů, které chcete vybrat.

V tomto příkladu vytvoříme nové pravidlo, které povolí aplikaci webového prohlížeče Firefox přistupovat k webovým stránkám internetu/místní síť:

1.V sekci **Akce** vyberte možnost **Akce > Povolit**.

2.V sekci **Aplikace** zadejte **Cestu k aplikaci** webového prohlížeče (např. C:\Program Files\Firefox\Firefox.exe). Nezadávejte pouze samotný název aplikace.

3.V sekci **Směr** vyberte možnost **Směr > Ven**.

4.V sekci **IP protokol** vyberte z rozbalovacího menu **Protokol TCP a UDP**.

5.V sekci **Vzdálený port** přidejte čísla **portů: 80,443** pro standardní internetové procházení.

Detekce změn aplikací

Funkce detekce změn aplikací zobrazí upozornění v případě, kdy se změněná aplikace, pro kterou existuje pravidlo brány firewall, pokusí navázat komunikaci. Změna aplikace je mechanismus dočasněho nebo trvalého nahrazení původní aplikace novou aplikací za pomoci jiného spustitelného souboru (chrání před zneužitím pravidel brány firewall).

Tato funkce není určena pro detekci změn všech aplikací. Cílem této funkce je zabránit zneužití existujících pravidel firewallu, proto jsou monitorovány pouze aplikace, pro které existují pravidla.

Chcete-li upravit **Detekce změn aplikací**, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Firewall** > **Detekce změn aplikací**.

Kontrolovat změnu aplikací – pokud je tato možnost aktivní, program bude sledovat, zda se daná aplikace změnila (aktualizovala, infikovala, jinak změnila). Hlášení o změně aplikace se zobrazí ve chvíli, kdy aplikace navazuje komunikaci.

Povolit změnu podepsaných (důvěryhodných) aplikací – o změně aplikací, které jsou digitálně podepsány nebudete informováni.

Seznam aplikací vyloučených z detekce – v tomto okně můžete přidávat nebo odebírat jednotlivé aplikace, u nichž je povolen provádět změny bez oznámení.

Seznam aplikací vyloučených z detekce

Firewall produktu ESET Smart Security Premium detekuje změny aplikací, pro které existuje pravidlo. Pro více informací přejděte do kapitoly [Detekce změn aplikací](#).

Pokud nechcete, aby konkrétní aplikace, pro kterou existuje pravidlo ve firewallu, byla sledována, můžete ji z monitorování vyloučit.

Přidat – po kliknutí se zobrazí dialogové okno, ve kterém můžete definovat aplikaci, kterou chcete vyloučit z detekce změn. Aplikaci můžete vybrat z již existujícího seznamu, které běží v systému a existuje pro ně pravidlo ve firewallu, případně zadejte cestu k aplikaci ručně.

Změnit – po kliknutí se zobrazí dialogové okno, ve kterém můžete upravit existující výjimku pro aplikaci vyloučenou z detekce změn. Jinou aplikaci si můžete vybrat z již existujícího seznamu, které běží v systému a existuje pro ně pravidlo ve firewallu, případně zadejte cestu k aplikaci ručně.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu aplikací vyloučených z detekce změn.

Ochrana proti síťovým útokům (IDS)

Ochrana proti síťovým útokům (IDS) zlepšuje detekci zneužití známých zranitelností. Více informací o tomto typu ochrany se můžete dočíst ve [slovníku pojmů](#). Chcete-li nakonfigurovat ochranu proti síťovým útokům, otevřete [Rozšířená nastavení](#) > **Ochrana** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům**.

Zapnout ochranu proti síťovým útokům (IDS) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Komunikace, která bude vyhodnocena jako škodlivá, bude blokována.

Zapnout ochranu proti zapojení do botnetu – funkce dokáže na základě typických vzorů detekovat a zablokovat komunikaci mezi škodlivým kódem ve vašem počítači a řídicími (C&C) servery botnetu. Více informací o této ochraně se můžete dočíst ve [slovníku pojmů](#).

IDS pravidla – umožňují nastavit pokročilé možnosti filtrování pro detekci několika typů útoků a zneužití, které by mohly poškodit váš počítač.

Názorné ukázky



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

- [Vyloučit IP adresu z IDS v ESET Smart Security Premium](#)

Všechny důležité události zaznamenané síťovou ochranou jsou ukládány do protokolů. Další informace naleznete v kapitole [Protokol síťové ochrany](#).

IDS pravidla

V některých případech může [Intrusion Detection Service \(IDS\)](#) detekovat komunikaci mezi routery nebo jinými interními síťovými zařízeními jako možný útok. Pokud je vám známá bezpečná adresa blokována, přidejte ji do Adres vyloučených z ochrany IDS pro obejití IDS.


Názorné ukázky



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

- [Vyloučit IP adresu z IDS v ESET Smart Security Premium](#)

Správa IDS pravidel

- **Přidat** – kliknutím vytvoříte nové IDS pravidlo.
- **Změnit** – kliknutím upravíte existující IDS pravidlo.
- **Odstranit** – kliknutím odstraníte existující pravidlo ze seznamu IDS pravidel.
-  **Šipky Nahoru/Výše/Dolů/Níže** – pomocí těchto tlačítek změníte pořadí vyhodnocování pravidel (výjimky jsou vyhodnocovány shora dolů).

IDS pravidla



IDS pravidla jsou vyhodnocovány shora dolů. Můžete je použít pro přizpůsobení chování firewallu při jednotlivých IDS detekcích. Pro každý typ akce se vždy pouze první vyhovující výjimka (blokovat, oznámit, zaznamenat do protokolu).

Detekce	Aplikace	Vzdálena IP	Blokovat	Oznámit	Zapsat do pro
<div> <div>Přidat</div> <div>Změnit</div> <div>Odstranit</div> </div> <div> <div>⌵</div> <div>⌴</div> <div>⌶</div> <div>⌷</div> </div>					

OK

Zrušit

Editor pravidel

Detekce – typ detekce.

Název hrozby – pro některé dostupné detekce můžete zadat název hrozby.

Aplikace – kliknutím na ... vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace.

Vzdálená IP adresa – seznam IPv4 nebo IPv6 adres / rozsahů adres / podsítí. Více záznamů oddělte čárkou.

Profil – můžete vybrat [profil síťového připojení](#), na který se toto pravidlo bude vztahovat.

Akce

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

Přidání IDS pravidla



Detekce

Jakákoli detekce

Název hrozby

Směr

Oba

Aplikace



Vzdálená IP adresa



Profil



Přidat

Odstranit

Akce

Blokovat

Výchozí akce

Oznámit

Výchozí akce

Zapsat do protokolu

Výchozí akce

OK

Zrušit

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 detekci.

3. Vyberte cestu aplikace kliknutím na ..., pro které chcete toto oznámení použít.

4. V rozbalovacím menu **Blokovat** ponechte možnost **Výchozí akce**. Tím se provede výchozí akce produktu ESET Smart Security Premium.

5. V rozbalovacím menu **Oznámit** a **Zapsat do protokolu** vyberte možnost **Ano**.

6. Oznámení uložte kliknutím na tlačítko **OK**.

Pokud nechcete pro konkrétní typy **Detekce**, které nepovažujete za hrozbu, zobrazovat opakovaná oznámení:

1. Klikněte na tlačítko **Přidat** pro vytvoření nového IDS pravidla.

2. Z rozbalovacího menu **Detekce** vyberte vámi požadovanou detekci, například **SMB relace bez bezpečnostního rozšíření** nebo **TCP Port Scanning attack**.

✓ 3. Jedná-li se o příchozí komunikaci, jako směr vyberte v rozbalovacím menu možnost **Dovnitř**.

4. V rozbalovacím menu **Oznámit** vyberte možnost **Ne**.

5. V rozbalovacím menu **Zapsat do protokolu** vyberte možnost **Ano**.

6. Pole **Aplikace** ponechte prázdné.

7. Pokud komunikace nepřichází pouze z konkrétní IP adresy, ponechte prázdné pole **Vzdálena IP adresa**.

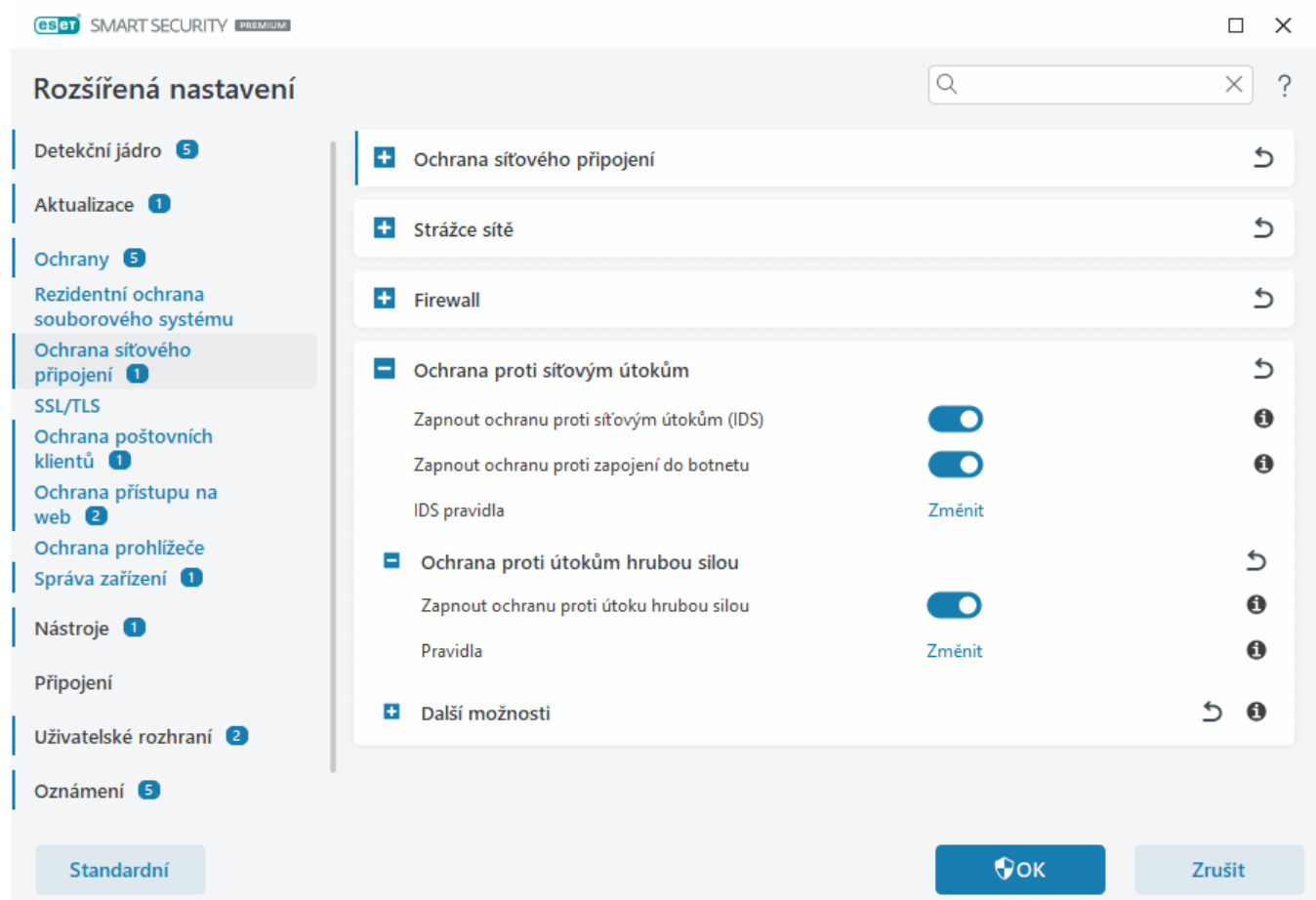
8. Oznámení uložte kliknutím na tlačítko **OK**.

Ochrana proti útokům hrubou silou

Ochrana proti útokům hrubou silou blokuje pokusy o uhádnutí hesel pro RDP a SMB služby. Útok hrubou silou je metoda, kdy se systematicky zkouší možné kombinace písmen, číslic a znaků za účelem prolomení hesla. Chcete-li nakonfigurovat Ochranu proti útokům hrubou silou, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Ochrana proti útokům hrubou silou**.

Zapnout ochranu proti útoku hrubou silou – tato součást produktu ESET Smart Security Premium 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](#).



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.

Změnit – kliknutím upravíte existující pravidlo..

Odstranit – kliknutím odstraníte existující pravidlo.



Nahoru/Výše/Dolů/Níže – umožní přizpůsobit pořadí vyhodnocování pravidel (vyhodnocovány jsou ze shora dolů).



Pro zajištění nejvyšší míry ochrany se pravidlo s nejnižším **maximálním počtem pokusů** uplatní i v případě, kdy se v seznamu nachází níže, než ostatní pravidla vyhovující podmínkám detekce.

Editor pravidel

eset SMART SECURITY PREMIUM ×

Přidat pravidlo ?

Název

Zapnuto ☒

Akce

Protokol

Profil i

PřidatOdstranit

Maximální počet pokusů i

Doba uchovávání adres na seznamu blokovanych i

Zdrojová IP adresa i

Sady zdrojových IP adres i

PřidatOdstranit

OKZrušit

Název – název pravidla.

Zapnuto – deaktivujte tuto možnost pomocí přepínače, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Akce – rozhodněte se, zda chcete při splnění pravidlem definovaných podmínek spojení **zamítnout** nebo **povolit**.

Protokol – informace, pro který síťový protokol pravidlo platí.

Profil – 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 blokovanych.


Doba uchovávání adres na seznamu blokovanych – definujte dobu, za jak dlouho bude adresa odstraněna ze seznamu blokovanych.


Zdrojová IP adresa – seznam IP adres, rozsahů nebo podsítí. Více záznamů oddělte čárkou.

Sady zdrojových IP adres – sada IP adres, které jste již definovali v [Sadách IP adres](#).

Rozšířená nastavení

V části [Rozšířená nastavení](#) > **Ochrany** > **Ochrana síťového připojení** > **Ochrana proti síťovým útokům** > **Další možnosti** můžete povolit nebo zakázat detekci několika typů útoků a exploitů, které mohou poškodit váš počítač.

 V některých případech neobdržíte oznámení o hrozbě týkající se blokové komunikace. Informace o tom, jak zobrazit veškerou zablokovanou komunikaci firewallem naleznete v kapitole [Protokolování a vytváření pravidel nebo výjimek z protokolu](#).

 Dostupnost jednotlivých možností závisí na typu a verzi produktu ESET, zda je vybaven firewallem, a stejně tak na verzi operačního systému.

Detekce útoků

Systém pro odhalení průniku vyhledává v síťové komunikaci škodlivou aktivitu.

- **Protokol SMB** – k dispozici jsou možnosti pro detekování a blokování mnoha zranitelností v SMB protokolu.
- **Protokol RPC** – detekce a blokování CVE v systémové službě vzdálené volání procedur určené pro Distributed Computing Environment (DCE).
- **Protokol RDP** – detekce a blokování CVE v RDP protokolu (viz výše).
- **Detekce útoku ARP Poisoning** – zabraňuje tzv. man-in-the-middle útokům a odhaluje odposlouchávání paketů síťových switchů, tedy stav, kdy útočník předává ostatním zařízením v síti falešné informace. ARP (Address Resolution Protocol) se používá při získávání a přiřazování IP adres zařízením v síti.
- **Detekce útoku skenování TCP/UDP portů** – zabraňuje útokům softwaru, který se pokouší zjistit otevřené porty v počítači, přes něž lze zařízení napadnout. Více o tomto typu útoku se můžete dočíst ve [slovníku pojmů](#).
- **Blokovat nebezpečnou adresu po detekci útoku** – IP adresy detekované jako zdroje útoků jsou přidány do seznamu blokových adres, aby se po určitou dobu zabránilo připojení. Můžete nastavit **Dobu uchování adres na seznamu blokových**, která nastavuje dobu, po kterou bude adresa po detekci útoku blokována.
- **Upozornit na detekci útoků** – po detekci útoku se zobrazí upozornění v pravém dolním rohu obrazovky v oznamovací oblasti.
- **Upozornit na příchozí útoky využívající bezpečnostní zranitelnosti** – k upozornění dojde, pokud bude zjištěn pokus o zneužití bezpečnostní díry, případně bude zaznamenán pokus o zneužití zranitelnosti k přístupu do systému.

Kontrola paketů

Vyberte si způsob analýzy paketů, která bude filtrovat data přenášená ve vaší síti.

- **Povolit příchozí spojení k administrativním sdílením prostřednictvím SMB protokolu** – administrativní sdílení jsou standardní síťová sdílení, které sdílí celé diskové oddíly (C\$, D\$, atd.) stejně jako systémové složky (ADMIN\$). Zakázáním připojení k administrátorským sdílením položkám snížíte bezpečnostní riziko. Například

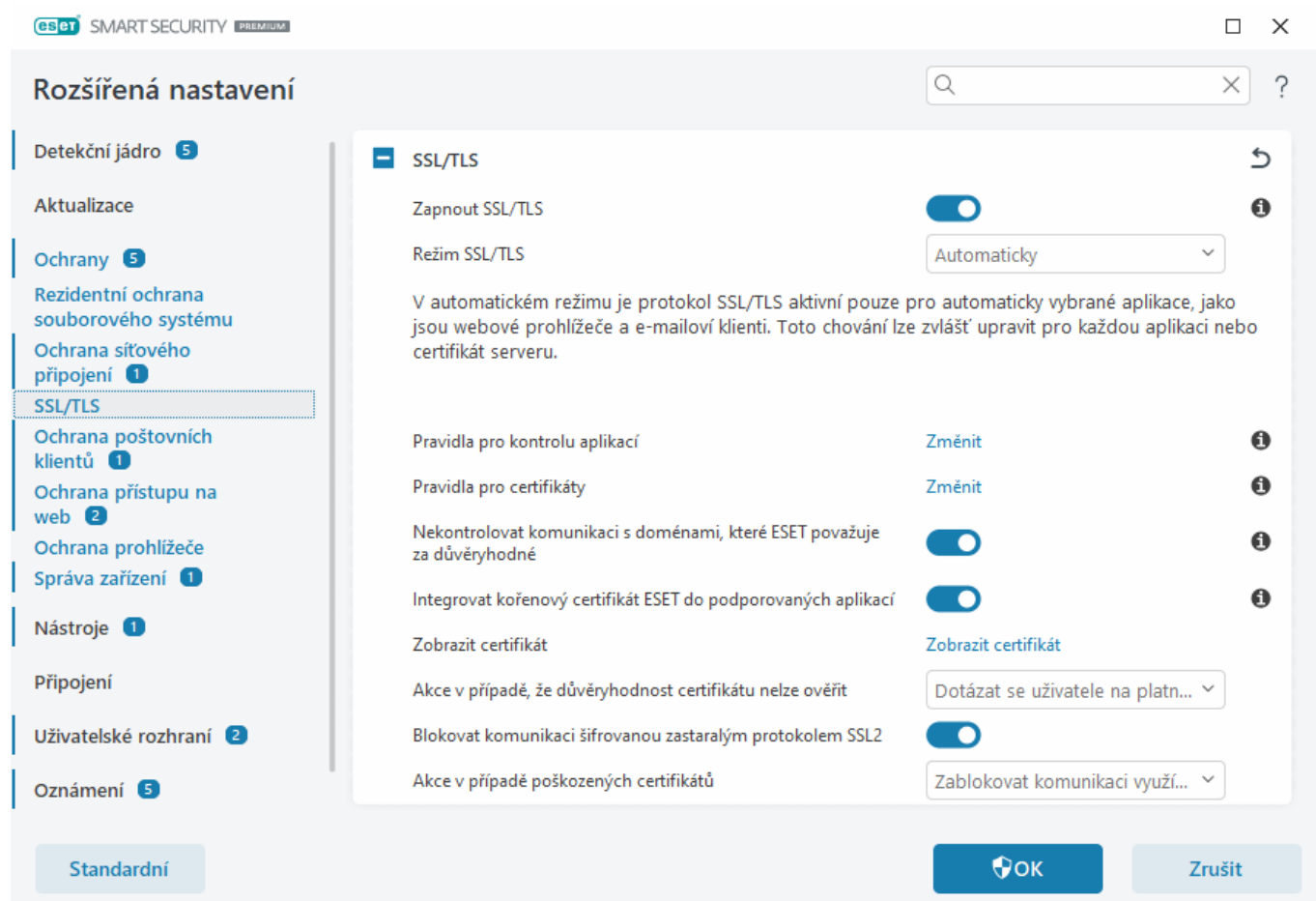
červ Conficker provádí slovníkový útok pro získání přístupu k administrátorským sdíleným položkám.

- **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 považováno za slabé a nedoporučuje se jej používat.
- **Zakázat otevření spustitelného souboru na serveru mimo Důvěryhodnou zónu pomocí SMB protokolu** – zabraňuje komunikaci v případě, že se snažíte otevřít spustitelný soubor (exe, dll) ze sdílené složky na serveru, který nepatří do důvěryhodné zóny definované ve firewallu. Mějte na paměti, že kopírování spustitelných souborů ze zdrojů v důvěryhodné zóně může být legitimní. Tato funkce by měla minimalizovat nebezpečí otevření nežádoucího souboru na škodlivém serveru, například když omylem kliknete na odkaz vedoucí na spustitelný soubor umístěný na sdíleném škodlivém serveru.
- **Zakázat NTLM autentifikaci pomocí SMB protokolu při připojení na server v/mimo Důvěryhodnou zónu** – protokoly využívající autentifikační schéma NTLM (obě verze) jsou ohrožené útoky přeposílajícími přihlašovací údaje (známé jako SMB relay útok v případě SMB protokolů). Zakázáním autentifikace NTLM se servery mimo důvěryhodnou zónu omezíte nebezpečí přeposílání přihlašovacích údajů škodlivým serverem mimo důvěryhodnou zónu. Můžete také zakázat NTLM autentifikaci se servery v důvěryhodné zóně.
- **Povolit komunikaci se službou Security Account Manager** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [\[MS-SAMR\]](#).
- **Povolit komunikaci se službou Local Security Authority** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [\[MS-LSAD\]](#) a [\[MS-LSAT\]](#).
- **Povolit komunikaci se službou Vzdálený registr** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [\[MS-RRP\]](#).
- **Povolit komunikaci se službou Správce řízení služeb** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [\[MS-SCMR\]](#).
- **Povolit komunikaci se službou Server** – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [\[MS-SRVS\]](#).
- **Povolit komunikaci s ostatními službami** – ostatní MSRPC služby. MSRPC je implementace DCE RPC mechanismu ve Windows. Kromě toho MSRPC může používat pojmenované roury pro SMB (síťové sdílení souborů) protokol. Služba MSRPC (Microsoft RPC) poskytuje přístup k rozhraní pro vzdálený přístup a ovládání systému Windows. V systému MSRPC bylo objeveno několik zranitelností, které zneužil například červ Conficker, červ Sasser, aj. Zakázáním komunikace s MSRPC službami, které nepotřebujete, minimalizuje bezpečnostní riziko (jako například vzdálené spouštění kódu po síti nebo pád služeb kvůli útoku).

SSL/TLS

ESET Smart Security Premium může kontrolovat komunikační hrozby, které používají SSL protokol. Filtrování můžete přizpůsobit podle toho, zda je certifikát využívaný danou SSL komunikací důvěryhodný, neznámý, nebo je

zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL. Chcete-li upravit nastavení SSL/TLS, otevřete [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS**.



Zapněte SSL/TLS – jestliže je vypnuto, ESET Smart Security Premium nebude kontrolovat komunikaci přes SSL/TLS.

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

Režim filtrování	Popis
Automaticky	Výchozí režim, ve kterém je kontrolována pouze komunikace vybraných aplikací, jako jsou webové prohlížeče a poštovní klienti. Můžete jej přepsat výběrem aplikací, u kterých se komunikace kontroluje.
Interaktivní	Při přístupu k nové stránce zabezpečené protokolem SSL (s neznámým certifikátem) se zobrazí dialogové okno s výběrem akce. V tomto režimu můžete vytvořit seznam SSL certifikátů / aplikací, které chcete vyloučit z kontroly.
Administrátorský režim	Tuto možnost vyberte, pokud chcete kontrolovat veškerou komunikaci zabezpečenou protokolem SSL kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru s nedůvěryhodným certifikátem označeným jako důvěryhodný (je v seznamu důvěryhodných certifikátů) je komunikace se serverem povolena a obsah komunikačního kanálu je filtrován.

Pravidla pro kontrolu aplikací – umožňují přizpůsobit chování ESET Smart Security Premium pro konkrétní aplikace.

Pravidla pro certifikáty – umožňují přizpůsobit chování ESET Smart Security Premium pro konkrétní SSL

certifikáty.

Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné – pokud je tato volba povolena, bude komunikace s důvěryhodnými doménami vyloučena z kontroly. Vestavěný seznam povolených adres spravovaný společností ESET určuje důvěryhodnost domény.

Integrovat kořenový certifikát ESET do podporovaných aplikací – aby SSL komunikace správně fungovala ve vašich prohlížečích a e-mailových klientech, je nezbytné, aby byl kořenový certifikát společnosti ESET přidán do seznamu známých kořenových certifikátů (vydavatelů). Pokud je tato možnost zapnutá, ESET Smart Security Premium automaticky přidá certifikát ESET SSL Filter CA do známých prohlížečů ve vašem počítači (např. do prohlížeče Opera). Do prohlížečů využívajících systémové úložiště kořenových certifikátů se certifikát přidá automaticky. Např. Firefox je automaticky nastaven tak, aby důvěřoval kořenovým autoritám nacházejícím se v systémovém úložišti certifikátů.

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

Akce v případě, že důvěryhodnost certifikátu nelze ověřit – v některých případech nelze certifikát webové stránky ověřit pomocí TRCA (Trusted Root Certification Authorities), například vypršela platnost certifikátu, certifikát není důvěryhodný, certifikát není platný pro danou doménu nebo podpis, který lze zpracovat, ale nepodepisuje správně. Legitimní webové stránky vždy používají důvěryhodné certifikáty. Pokud je neposkytují, může to znamenat, že útočník dešifruje vaši komunikaci nebo že webové stránky mají technické potíže.

Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (ve výchozím nastavení je vybrána), při navázání šifrované komunikace se zobrazí okno s výběrem akce. V zobrazeném dialogovém okně pro výběr akce můžete certifikát označit jako důvěryhodný nebo vyloučený. Pokud se certifikát nenachází v TRCA, okno bude červené. V opačném případě bude okno zelené.

Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** vždy zablokujete komunikaci s webovou stránkou využívající nedůvěryhodný certifikát.

Blokovat komunikaci šifrovanou zastaralým protokolem SSL2 – komunikace pomocí starší verze protokolu SSL bude automaticky blokována.

Akce v případě poškozených certifikátů – poškozený certifikát znamená, že certifikát používá formát, který ESET Smart Security Premium nerozpoznává, nebo byl přijat poškozený (například přepsaný náhodnými daty). V tomto případě doporučujeme ponechat zvolenou možnost **Zakázat komunikaci využívající daný certifikát**. Pokud vyberete **Dotázat se uživatele na platnost certifikátů**, uživatel bude vyzván k výběru akce po navázání šifrované komunikace.

Názorné příklady

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



- [Upozornění na certifikát v produktu ESET](#)
- [Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"](#)

Pravidla pro kontrolu aplikací

Pomocí **Pravidel pro kontrolu aplikací** můžete přizpůsobit chování ESET Smart Security Premium u konkrétních aplikací a zapamatovat si vybrané akce, pokud je **Režim filtrování protokolu SSL/TLS** nastaven v **Interaktivním režimu**. Seznam lze zobrazit a upravit v části [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS** > **Pravidla pro kontrolu**

aplikací > Změnit.

Okno **Pravidla pro kontrolu aplikací** se skládá z:

Sloupce

Aplikace – vyberte spustitelný soubor kliknutím na ... nebo zadejte cestu k souboru ručně.

Akce při kontrole – pro kontrolu nebo ignorování komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – kliknutím přidáte filtrovanou aplikaci.

Změnit – vyberte aplikaci, kterou chcete konfigurovat a klikněte na tlačítko **Změnit**.

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

Importovat/Exportovat – seznam aplikací můžete importovat ze souboru, případně si jej a uložit pro budoucí použití.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

Pravidla pro certifikáty

Pravidla pro certifikáty lze použít k přizpůsobení chování ESET Smart Security Premium pro konkrétní certifikáty SSL a k zapamatování akcí zvolených v režimu **SSL/TLS** v **interaktivním režimu**. Seznam lze zobrazit a upravit v části [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS** > **Pravidla pro certifikáty** > **Změnit**.

Okno **Pravidla pro certifikáty** se skládá z:

Sloupce

Název – název certifikátu.

Vydavatel certifikátu – jméno autora certifikátu.

Předmět certifikátu – identifikace entity asociované s veřejným klíčem uloženým v poli předmět veřejného klíče.

Akce při přístupu – pro **povolení** nebo **zablokování** komunikace využívající daný certifikát bez ohledu na to, zda je důvěryhodný, vyberte možnost **Povolit** nebo **Blokovat**. V případě možnosti **Automaticky** budou důvěryhodné certifikáty povoleny, a v případě nedůvěryhodných bude muset uživatel vybrat akci. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Akce při kontrole – pro **kontrolu** nebo **ignorování** komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**,

vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – certifikát můžete přidat ručně ve formátu .cer, .crt nebo .pem a to buď přímo ze souboru nebo externího zdroje po zadání URL.

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

Odstranit – vyberte certifikát, který chcete smazat a klikněte na tlačítko **Odstranit**.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

Šifrovaná síťová komunikace

Pokud je váš systém nakonfigurován tak, aby kontroloval SSL/TLS, zobrazí se dialogové okno s výzvou k výběru akce ve dvou situacích:

Webová stránka používá neověřený nebo neplatný certifikát a ESET Smart Security Premium je nakonfigurován tak, aby se dotázal uživatele (standardně je tato možnost aktivní pro neověřené certifikáty, nikoli neplatné), zda chcete komunikaci **Povolit** nebo **Zakázat**. Pokud se certifikát nenachází v Trusted Root Certification Authorities store (TRCA), je považován za nedůvěryhodný.

Za druhé, pokud je **režim SSL/TLS** nastaven na **Interaktivní**, zobrazí se u každé webové stránky dialogové okno s dotazem, zda se má komunikace **Kontrolovat** nebo **Ignorovat**. Některé aplikace ověřují, že jejich SSL nikdo nemodifikuje ani nekontroluje, v takových případech musí ESET Smart Security Premium tuto komunikaci **ignorovat**, aby aplikace fungovala.

Názorné příklady

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

- [Upozornění na certifikát v produktu ESET](#)
- [Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"](#)

V obou případech je dostupná možnost pro zapamatování vybrané akce. Zapamatované akce jsou uloženy v [Pravidlech pro certifikáty](#).

Ochrana poštovních klientů

Chcete-li nastavit Ochranu poštovních klientů, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** a vyberte jednu z následujících možností:

- [Ochrana transportu zpráv](#)
- [Ochrana poštovní schránky](#)
- [Správa seznamů adres](#)
- [ThreatSense](#)

Ochrana transportu zpráv

POP3(S) a IMAP(S) jsou nejrozšířenější protokoly určené pro příjem e-mailové komunikace prostřednictvím poštovního klienta. Internet Message Access Protocol (IMAP) je další internetový protokol pro získávání pošty. IMAP má oproti POP3 několik výhod, například více klientů se může současně připojit ke stejné poštovní schránce a udržovat informace o stavu zprávy (např. zda byla zpráva přečtena, zda na ni bylo odpovězeno nebo byla odstraněna. Modul ochrany poskytující tuto kontrolu je automaticky zaveden při spuštění systému a je pak aktivní v paměti.

ESET Smart Security Premium 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.

i ESET Smart Security Premium rovněž podporuje kontrolu protokolů IMAPS (585, 993) a POP3S (995), které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Smart Security Premium kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Šifrovaná komunikace se standardně nekontroluje. Chcete-li zobrazit nastavení skeneru, otevřete [Rozšířená nastavení](#) > **Ochrany** > [SSL/TLS](#).

Chcete-li nakonfigurovat ochranu přenosu pošty, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana transportu zpráv**.

Povolit ochranu transportu zpráv – pokud je tato ochrana povolena, bude ESET Smart Security Premium kontrolovat poštovní komunikaci.

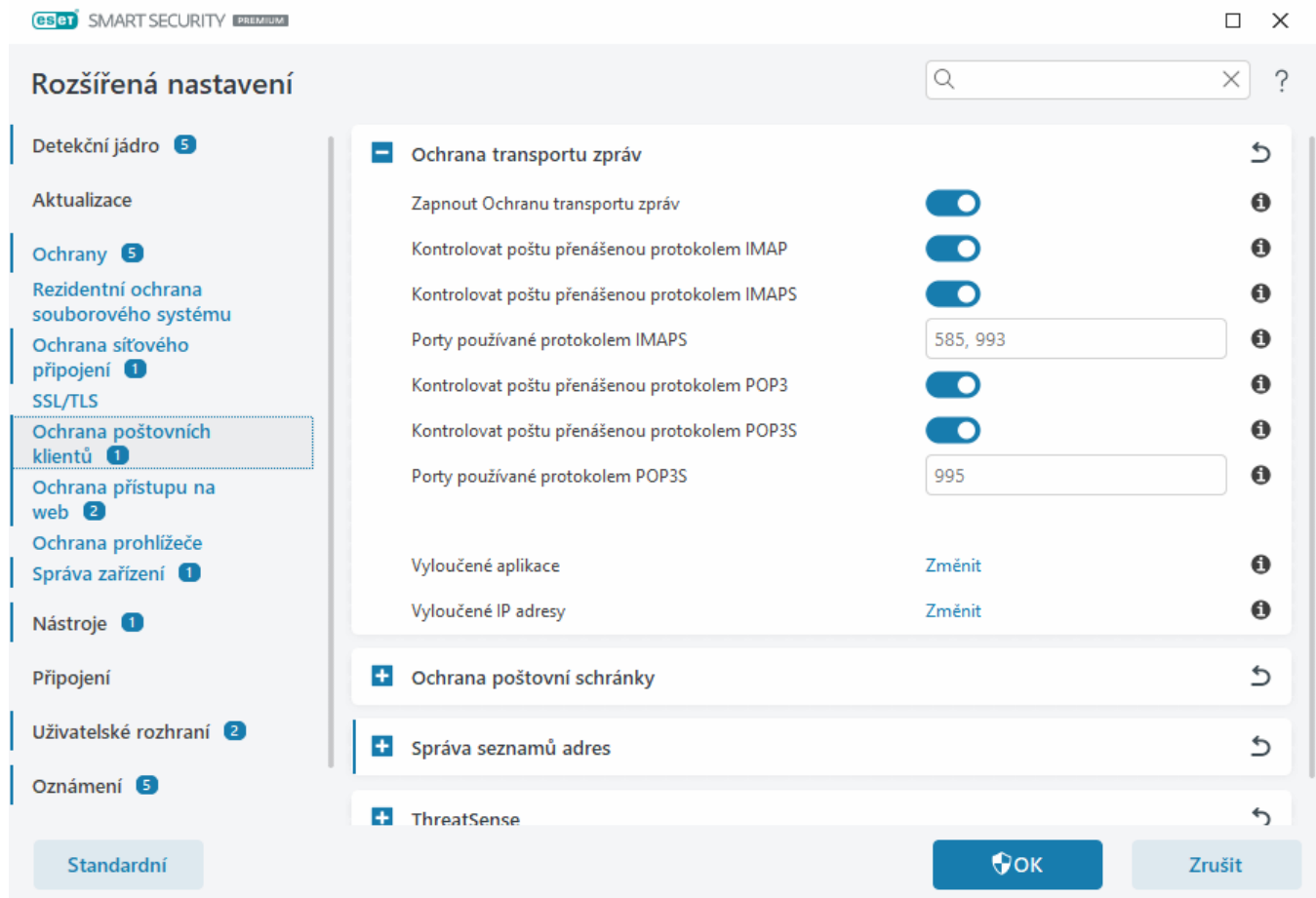
Kliknutím na přepínač vedle následujících možností můžete zvolit, které protokoly pro přenos pošty budou kontrolovány (ve výchozím nastavení je povolena kontrola všech protokolů):

- **Kontrolovat poštu přenášenou protokolem IMAP**
- **Kontrolovat poštu přenášenou protokolem IMAPS**
- **Kontrolovat poštu přenášenou protokolem POP3**
- **Kontrolovat poštu přenášenou protokolem POP3S**

Ve výchozím nastavení bude ESET Smart Security Premium kontrolovat komunikaci na standardních portech IMAPS a POP3S. Chcete-li přidat vlastní porty pro protokoly IMAPS a POP3S, zadejte je do textového pole vedle **Porty používané protokolem IMAPS** nebo **Porty používané protokolem POP3S**. Více čísel portů je třeba oddělit čárkou.

[Vyloučené aplikace](#) – umožňuje neprovádět Ochranu poštovního transportu u zvolených aplikací. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

[Vyloučené IP adresy](#) – umožňuje neprovádět u konkrétních adres kontrolu pomocí Ochrany transportu zpráv. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



Vyloučené aplikace

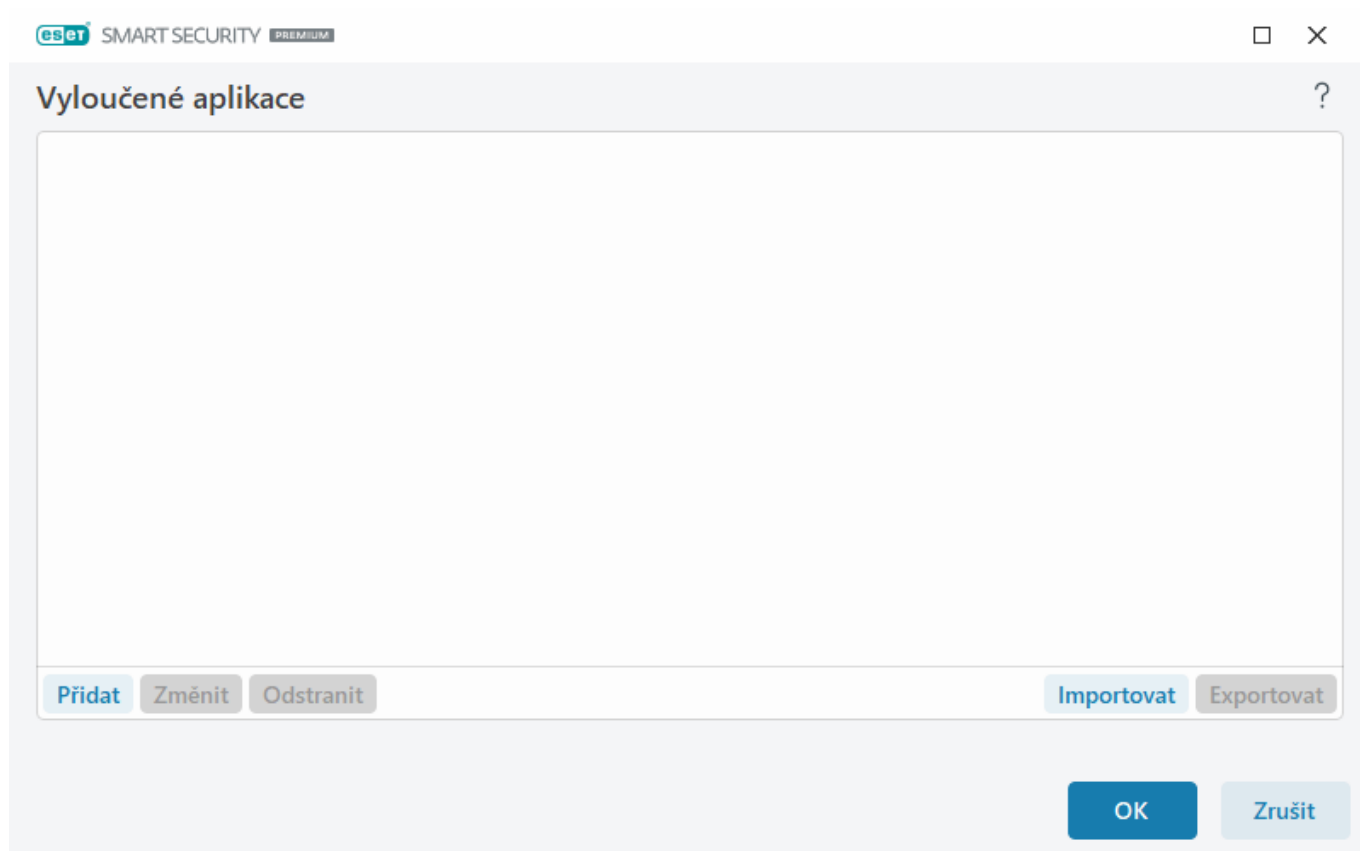
Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu.

HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na ... a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



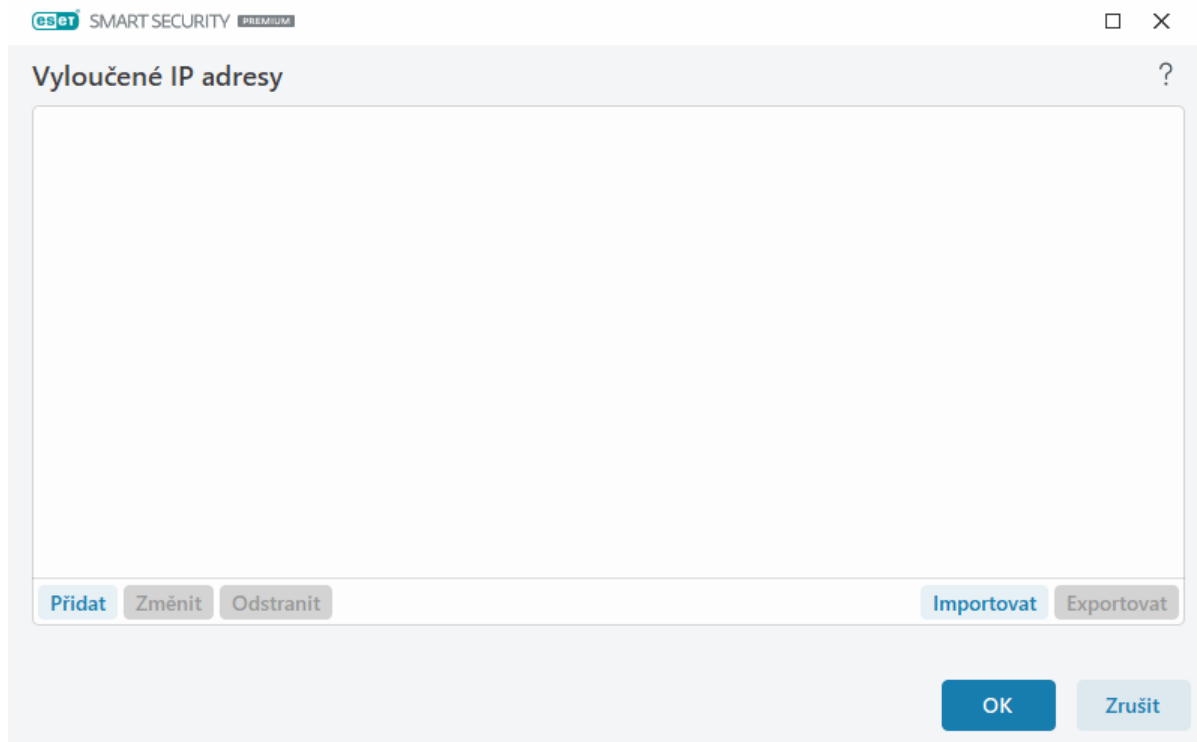
Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany.

Upravit – klikněte pro změnu vybrané IP adresy.

Odstranit – kliknutím odstraníte vybrané IP adresy ze seznamu.



Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).

Rozsah adres – umožní zadat počáteční a koncovou IP adresu pro rozsah IP adres několika zařízení (například *192.168.0.1-192.168.0.99*).

✓ **Podsít** – umožní zadat podsít skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsít 192.168.1.0. Chcete-li vyloučit celou podsít, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsít – podsít skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Ochrana poštovní schránky

Integrace ESET Smart Security Premium s poštovní schránkou zvyšuje úroveň ochrany před škodlivým kódem v e-mailových zprávách.

Chcete-li nakonfigurovat ochranu poštovní schránky, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky**.

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

Vyberte e-maily pro kontrolu:

- Příchozí zprávy
- Odchozí zprávy
- Čtené zprávy

- **Změněná zpráva**

i Doporučujeme, abyste možnost **Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta** měli zapnutou. I když integrace není zapnuta nebo je nefunkční, ochrana e-mailové komunikace je stále zajišťována prostřednictvím modulu [Ochrana transportu zpráv](#) (IMAP/IMAPS a POP3/POP3S).

Vyhledávání spamu

V současnosti mezi největší problémy e-mailové komunikace patří nevyžádaná pošta. Spam představuje více než 30 % veškeré e-mailové komunikace. Antispamová ochrana poštovních klientů chrání před tímto problémem. Kombinuje několik principů zabezpečení e-mailů a poskytuje vynikající filtrování, aby vaše doručená pošta zůstala čistá. Pro detekci spamu je jedním z důležitých principů rozpoznávání nevyžádaných e-mailů na základě předdefinovaných důvěryhodných adres (povolených) a spamových adres (blokových).

Hlavním principem je rozpoznávání spamu na základě vlastností e-mailových zpráv. Přijatá zpráva je prověřena na základě pravidel (vzorky zpráv, statistická heuristika, rozpoznávací algoritmy a další jedinečné metody) a podle výsledku se rozhodne, zda se jedná o spam nebo ne.

Povolit Antispamovou ochranu poštovních klientů – pokud je tato funkce povolena, budou přijaté zprávy kontrolovány na přítomnost spamu.

Použít pokročilou kontrolu spamu – pravidelně se budou stahovat další antispamová data, čímž se zvyšují antispamové schopnosti a dosahuje se lepších výsledků.

Zapisovat skóre antispamové ochrany do protokolu – antispamové jádro ESET Smart Security Premium přiřazuje každé zkontrolované zprávě skóre. Zpráva je zároveň zaznamenána do [protokolu antispamové ochrany](#), který je dostupný v [hlavním okně programu](#) na záložce **Nástroje > Protokoly > Antispamová ochrana poštovních klientů**.

- **Nezapisovat** – sloupec Skóre bude v protokolu antispamové ochrany prázdný.
- **Zapisovat pouze pro přehodnocené zprávy a zprávy označené jako SPAM** – vyberte tuto možnost, pokud chcete zapisovat spam skóre pouze pro zprávy označené jako SPAM.
- **Zapisovat pro všechny zprávy** – všechny zprávy budou mít zaznamenáno spam skóre.

i Po kliknutí pravým tlačítkem na zprávu umístěnou ve složce spam můžete z kontextového menu vybrat možnost **Přehodnotit vybrané zprávy jako NENÍ spam**. Zpráva bude přemístěna do složky s doručenou poštou. Po kliknutí pravým tlačítkem na zprávu umístěnou ve složce doručené pošty můžete z kontextového menu vybrat možnost **Přehodnotit vybrané zprávy jako spam**. Zpráva bude přemístěna do složky s nevyžádanou poštou. Můžete vybrat více zpráv a provést akci na všech z nich současně.

Optimalizovat zpracování příloh – při vypnutí této možnosti budou všechny přílohy kontrolovány okamžitě. Může tím dojít ke zpomalení výkonu e-mailového klienta.

Integrace – umožňuje integrovat Ochranu poštovní schránky do e-mailového klienta. Další informace naleznete v kapitole [Integrace](#).

Reakce – umožňuje přizpůsobit zpracování nevyžádaných zpráv. Další informace naleznete v kapitole [Reakce](#).

Integrace

Integrace ESET Smart Security Premium do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdržným prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET Smart Security Premium podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET Smart Security Premium do poštovního klienta, což přispívá k efektivnější kontrole e-mailových zpráv. Chcete-li upravit nastavení integrace, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Integrace**.

Povolit integraci s Microsoft Outlook – [Microsoft Outlook](#) je v současné době jediným podporovaným e-mailovým klientem. Poštovní ochrana je zajišťována pomocí doplňku. Hlavní výhodou doplňku je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Úplný seznam podporovaných poštovních klientů a jejich verzí naleznete v [ESET Databázi znalostí](#) (článek nemusí být dostupný ve všech jazycích).

Pokročilé zpracování poštovními klienty – zpracovává další [Outlook Messaging API \(MAPI\) události](#): Objekt upraven (`fnevObjectModified`) a Objekt vytvořen (`fnevObjectCreated`). Tuto možnost vypněte, pokud pozorujete propad výkonu při práci s vaším poštovním klientem.

Panel nástrojů v MS Outlook

Ochrana Microsoft Outlook pracuje jako zásuvný modul (plug-in). Po instalaci ESET Smart Security Premium se do aplikace Microsoft Outlook přidá tento panel nástrojů s možnostmi pro antivirovou ochranu a Antispamovou ochranou poštovních klientů:

Spam – umožňuje vybrané zprávy označit jako spam. Po označení se odešle "otisk" zprávy na centrální server s databází charakteristik nevyžádané pošty. V případě, že stejný "otisk" odešle větší počet uživatelů, bude tato zpráva v budoucnu vyhodnocena jako spam.

Není spam – umožňuje vybrané zprávy označit jako není spam.

Spamová adresa (seznam spamových adres, tzv. blacklist) – přidá adresu odesílatele [na seznam spamových adres](#) jako Blokováno. Všechny zprávy přijaté z těchto adres budou automaticky označovány jako spam.



Při odesílání nevyžádané pošty se využívá tzv. spoofing, kdy se skutečný odesílatel maskuje za jinou e-mailovou adresu. Buďte tedy obezřetní.

Důvěryhodná adresa (Povoleno, seznam důvěryhodných adres, tzv. whitelist) – přidá adresu odesílatele vybraných zpráv na [Seznam důvěryhodných adres](#) jako Povoleno. Zprávy z těchto adres nebudou nikdy automaticky označovány jako spam.

ESET Smart Security Premium – dvojitým kliknutím na ikonu otevřete hlavní okno programu ESET Smart Security Premium.

Znovu zkontrolovat zprávy – umožní ruční spuštění kontroly e-mailů. V této části můžete vybrat zprávy, které budou zkontrolovány. Tím můžete aktivovat opakovanou kontrolu přijatého e-mailu. Další informace naleznete v kapitole [Ochrana poštovní schránky](#).

Nastavení skeneru – zobrazí možnosti nastavení [ochrany poštovní schránky](#).

Nastavení antispamu – zobrazí možnosti nastavení [ochrany poštovní schránky](#).

Seznamy adres – otevře okno [Správa seznamů adres](#), kde můžete přistupovat k seznamům vyloučených, důvěryhodných a nevyžádaných adres.

Potvrzovací dialog

Dialog s možností potvrzení nebo zamítnutí dané akce slouží pro ověření, že chcete akci opravdu provést. Předejdete tím také akcím, jejichž provedení jste nastavili nedopatřením.

Zároveň můžete tato upozornění vyžadující potvrzení zcela vypnout.

Opakovaná kontrola zpráv

Na panelu nástrojů produktu ESET Smart Security Premium integrovaném v poštovním klientovi máte k dispozici možnosti pro kontrolu zpráv. Dostupné jsou dvě možnosti kontroly:

Všechny zprávy v aktuální složce – zkontrolují se všechny zprávy ve složce, která je aktuálně zobrazena.

Pouze označené zprávy – zkontrolují se pouze zprávy, které jste vybrali ručně.

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

Reakce

Na základě výsledků kontroly zpráv může ESET Smart Security Premium zkontrolované zprávy přesunout nebo přidat vlastní text do předmětu. Tato nastavení můžete provádět v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Reakce**.

Antispamová ochrana poštovních klientů v ESET Smart Security Premium umožňuje konfigurovat následující parametry zpráv:

Přidávat text do předmětu zprávy – umožňuje přidávat vlastní text do předmětu e-mailové zprávy klasifikované jako spam. Výchozí **text** je "[SPAM]".

Přesunout do spamové složky – po zapnutí této možnosti budou nevyžádané zprávy přesouvány do výchozí složky s nevyžádanou poštou a naopak, zprávy nevyhodnocené jako spam budou přesouvány do složky s doručenou poštou. Klikem pravým tlačítkem myši na e-mail a výběrem ESET Smart Security Premium z kontextového menu můžete rovněž vybrat, jaké povahy pošta je.

Přesunout do vlastní složky – pokud je tato možnost povolena, budou nevyžádané zprávy přesunuty do níže uvedené složky.

Složka – definujte vlastní složku, do které přesouvat infikované zprávy.

Pokud zpráva obsahuje detekci, ve výchozím nastavení se ji ESET Smart Security Premium pokusí vyléčit. Pokud zprávu nelze vyléčit, můžete zvolit **Akce, pokud není možné objekt vyléčit**:

- **Žádná akce** – program upozorní na zprávy s infikovanými přílohami, avšak neprovede žádnou akci.
- **Odstranit zprávu** – program upozorní na infikované přílohy a odstraní celou zprávu.
- **Přesunout zprávu do složky s odstraněnými zprávami** – program bude přesouvat infikované zprávy do složky s vymazanými zprávami.
- **Přesunout zprávu do složky (výchozí akce)** – program bude přesouvat infikované zprávy do vybrané složky.

Složka – vlastní složka, do které se mají přesouvat infikované e-maily.

Označit SPAM zprávy jako přečtené – po aktivování této možnosti se nevyžádaná zpráva označí jako přečtená. To vám pomůže koncentrovat pozornost na legitimní "čisté" doručené zprávy.

Přehodnocené zprávy označit jako nepřečtené – zprávy, které byly dříve označeny jako spam, budou po novém vyhodnocení jako legitimní označeny jako nepřečtené.

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do příchozích a čtených zpráv** nebo **Přidávat do odchozích zpráv**. Samozřejmě, na tyto podpisy se nelze zcela spoléhat, protože nemusí být doplněny do problematických HTML zpráv a také mohou být zfalšovány malwarem. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy nebo pro oboje. K dispozici jsou následující možnosti:

- **Nikdy** – program nebude přidávat podpisy,
- **Při výskytu detekce** – pouze zprávy obsahující škodlivý software budou označeny jako zkontrolované (výchozí).
- **Přidávat do všech kontrolovaných zpráv** – program bude přidávat zprávy do všech kontrolovaných e-mailů.

Modifikovat předmět příchozích a čtených zpráv / Modifikovat předmět odchozích zpráv – povolením této možnosti přidáte do zprávy vlastní text zadaný níže.

Šablona přidávaná do předmětu infikovaných zpráv – upravte tuto šablonu, pokud chcete změnit formát předpony předmětu infikovaného e-mailu. Tato funkce přidá k původnímu předmětu zprávy "Ahoj" předponu "[detekce %DETECTIONNAME%]". Proměnná %DETECTIONNAME% představuje detekovanou hrozbu.

Správa seznamů adres

Antispamová ochrana poštovních klientů v ESET Smart Security Premium umožňuje nastavit různé parametry pro práci se seznamem adres. Chcete-li nakonfigurovat seznamy adres, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Správa seznamů adres**.

Povolit uživatelský seznam adres – pomocí této možnosti povolíte na tomto zařízení používání uživatelského seznamu adres.

Uživatelský seznam adres – po kliknutí na Změnit se zobrazí [editor pravidel antispamové ochrany](#). Pravidla definovaná v tomto seznamu jsou platná pro aktuálně přihlášeného uživatele.

Povolit globální seznam adres – pomocí této možnosti povolíte používání globálního seznamu adres, který bude sdílený se všemi uživateli na tomto zařízení.

Globální seznam adres – po kliknutí na Změnit se zobrazí [editor pravidel antispamové ochrany](#). Pravidla definovaná v tomto seznamu se aplikují na všechny uživatele.

Automatické povolení a přidávání do uživatelského seznamu adres

Považovat adresy ze seznamu kontaktů za důvěryhodné – pokud je tato možnost aktivní, adresy z vašeho seznamu kontaktů budou považovány za důvěryhodné, aniž by se nacházely na uživatelském seznamu adres.

Přidávat adresy příjemců z odesílaných zpráv – po aktivování této možnosti se na [seznam povolených adres](#) přidají všechny adresy příjemců, kterým jste zaslali e-mail.

Přidávat adresy odesílatelů ze zpráv klasifikovaných jako NENÍ SPAM – po aktivování této možnosti se na [seznam povolených adres](#) přidají adresy odesílatelů zpráv, které byly přehodnocené jako NENÍ SPAM.

Automatické přidávání do uživatelského seznamu adres jako výjimky

Přidávat adresy z vlastních účtů – umožní přidání e-mailových adres z poštovního klienta do uživatelského seznamu adres jako [výjimky](#).

Seznamy adres

Pro zajištění ochrany před nevyžádanými e-maily vám ESET Smart Security Premium umožňuje definovat seznamy e-mailových adres.

Chcete-li upravit seznamy adres, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Správa seznamů adres** a klikněte na tlačítko **Změnit** vedle položky **Uživatelský seznam adres** nebo **Globální seznam adres**.

E-mailová adresa	Název	Povolit	Bloko...	Výjimka	Poznámka
mary@marymail.com	Mary Smith	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	přidáno ručně
@address.info	John Smith	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	celá doména, přidáno ručně
@verygoodnews.net	Newsletter	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	celá doména, domény nižších řádů, př...

Přidat Změnit Odstranit

OK Zrušit

Sloupce

E-mailová adresa – adresa, na kterou se bude pravidlo vztahovat. Zástupné znaky nejsou podporovány.

Název pravidla – název vámi definovaného pravidla.

Povolit/Blokovat/Výjimka – pole používaná k určení, jakou akci provést pro e-mailovou adresu (kliknutím na pole v upřednostňovaném sloupci akci rychle změníte):

- **Povolit** – Adresy, které považujete za důvěryhodné a chcete z nich vždy dostávat e-maily.
- **Blokovat** – Adresy, které považujete za nedůvěryhodné/spam a ze kterých nechcete dostávat e-maily.
- **Výjimka** – Adresy, které jsou vždy kontrolovány pro možný výskyt spamové pošty a které mohou být zfalšovány a použity pro jeho odesílání.

Poznámka – informace o tom, kým bylo pravidlo vytvořeno, a zda se vztahuje na celou doménu / domény nižší úrovně.

Správa adres

- **Přidat** – kliknutím přidáte pravidlo pro novou adresu.
- **Změnit** – kliknutím upravíte existující pravidlo.
- **Odstranit** – kliknutím odstraníte existující pravidlo ze seznamu.

Přidat/Upravit záznam

Toto okno umožňuje přidat nebo upravit adresu ve [Správě seznamů adres](#) a definovat akci, která se má provést:

E-mailová adresa – adresa, na kterou se bude pravidlo vztahovat.

Název pravidla – název vámi definovaného pravidla.

Akce – Akce, která se má provést, pokud se e-mailová adresa kontaktu shoduje s adresou zadanou v poli **E-mailová adresa**:

- **Povolit** – Adresy, které považujete za důvěryhodné a chcete z nich vždy dostávat e-maily.
- **Blokovat** – Adresy, které považujete za nedůvěryhodné/spam a ze kterých nechcete dostávat e-maily.
- **Výjimka** – Adresy, které jsou vždy kontrolovány pro možný výskyt spamové pošty a které mohou být zfalšovány a použity pro jeho odesílání.

Celá doména – vybráním této možnosti se do seznamu zařadí celá doména daného kontaktu (ne jen **konkrétní e-mailová adresa**, ale všechny e-mailové adresy z domény například z *adresa.cz*).

Domény nižších řádů – vybráním této možnosti se do seznamu zařadí doména nižších řádů daného kontaktu (*adresa.cz* reprezentuje doménu, zatímco *moje.adresa.cz* subdoménu).

Výsledek zpracování adres

Při přidávání nebo [přesouvání e-mailových adres mezi seznamy povolených adres, spamových adres a seznamem výjimek](#) může ESET Smart Security Premium zobrazit oznámení. Obsah oznámení závisí na akci, kterou jste se pokoušeli provést.

Vybráním možnosti **Příště tuto zprávu nezobrazovat** se akce provede automaticky a okno se již příště nezobrazí.

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

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

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochrany 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 schopnosti produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizacího 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 Smart Security Premium během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET Smart Security Premium

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.
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.

Úroveň léčení	Popis
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 doporučeno 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 určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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 ji 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](#) zapíše 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 neoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty

doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena.

V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány.

Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik).

Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.


Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: **3 GB**.

 Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Ochrana přístupu na web

Ochrana přístupu na web umožňuje konfigurovat pokročilá nastavení modulu [Internetová ochrana](#). V [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana přístupu na web** > **Ochrana přístupu na web** jsou k dispozici následující možnosti:

Zapnout ochranu přístupu na web – pokud je tato možnost vypnutá, nefunguje Ochrana přístupu na web ani [Anti-Phishingová ochrana](#).

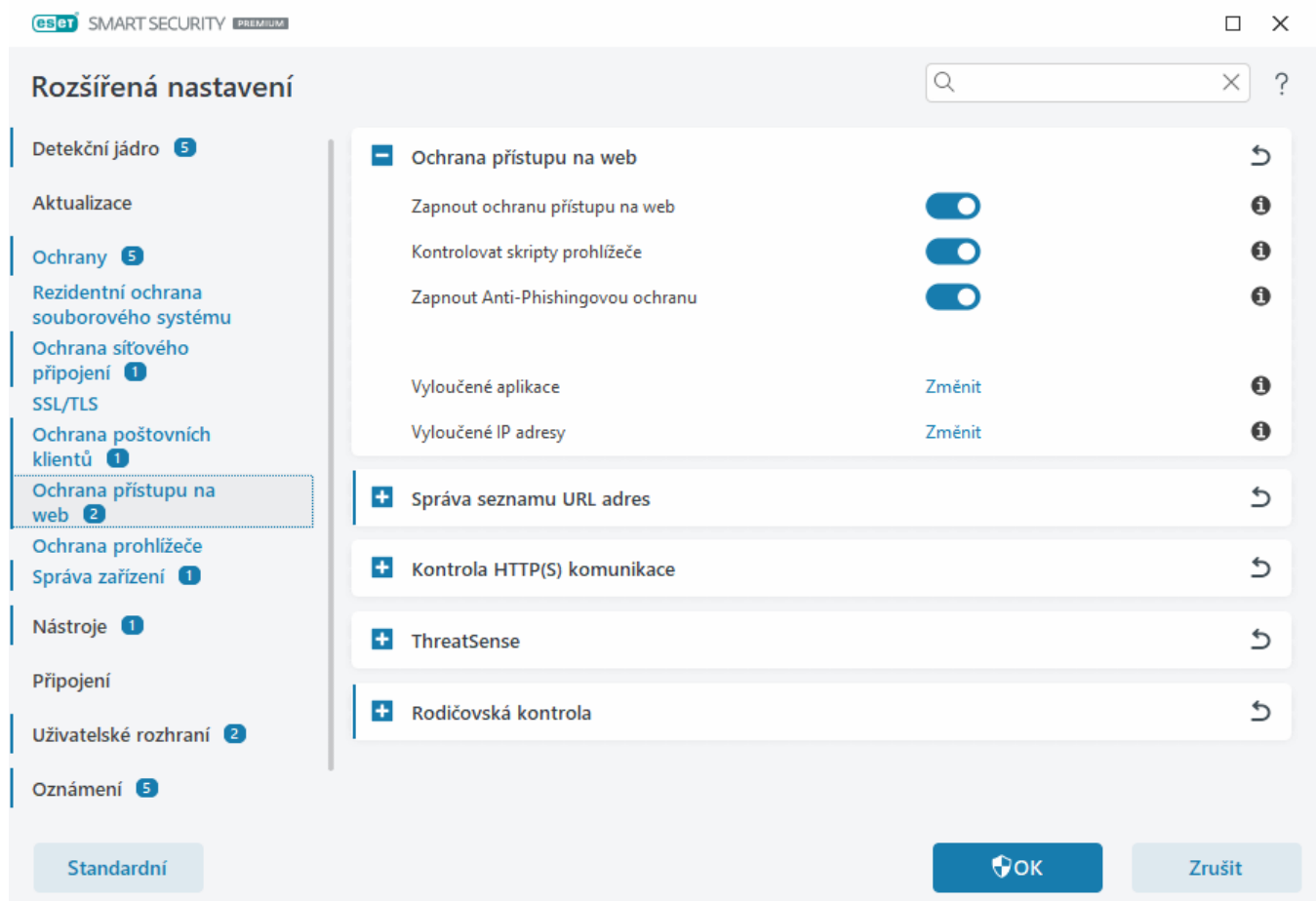
 Důrazně doporučujeme ponechat Ochranu přístupu na web zapnutou a nevylučovat žádné aplikace ani IP adresy ve výchozím nastavení.

Kontrolovat skripty prohlížeče – pokud je tato funkce povolena, detekční jádro zkontroluje všechny JavaScript programy spouštěné webovými prohlížeči.

Zapnout Anti-Phishingovou ochranu – pokud je povolena, jsou phishingové webové stránky blokovány. Pro více informací přejděte do kapitoly [Anti-Phishingová ochrana](#).

Vyloučené aplikace – umožňuje vyloučit konkrétní aplikace z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

Vyloučené IP adresy – umožňuje vyloučit konkrétní IP adresy z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



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



Nalezena hrozba

Stránka obsahuje potenciálně nebezpečný obsah.

Hrozba: HTML/ScrInject.B trojský kůň

Přístup na tuto stránku byl zablokován. Váš počítač je v bezpečí.

[Otevřít ESET Databázi znalostí](#) | www.eset.cz

Názorné ukázky



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

- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Jak zablokovat přístup na webovou stránku prostřednictvím produktu ESET Smart Security Premium](#)

Vyloučené aplikace

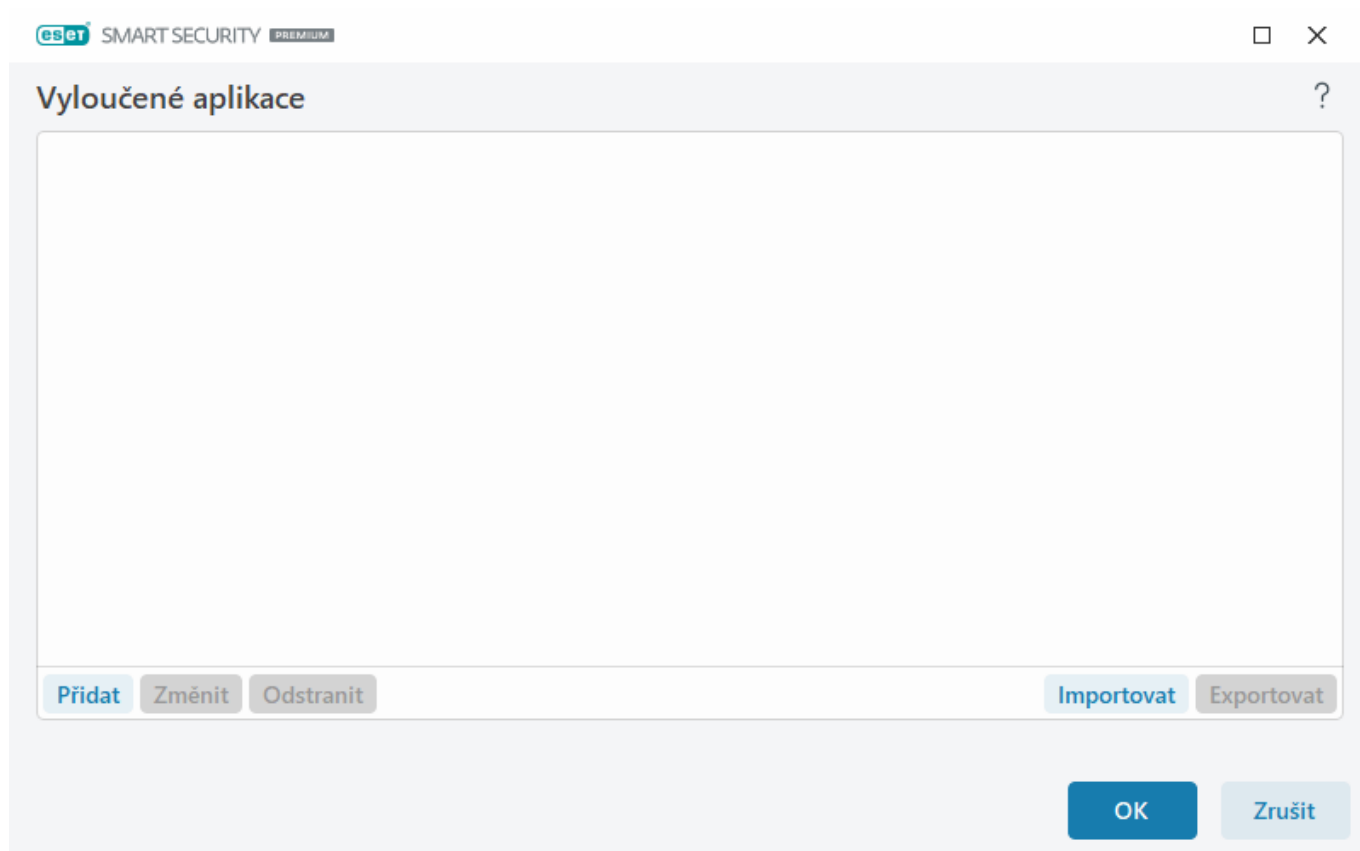
Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu.

HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na ... a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany.

Upravit – klikněte pro změnu vybrané IP adresy.

Odstranit – kliknutím odstraníte vybrané IP adresy ze seznamu.

Vyloučené IP adresy



--	--

Přidat

Změnit

Odstranit

Importovat

Exportovat

OK

Zrušit

Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).**Rozsah adres** – umožní zadat počáteční a koncovou IP adresu pro rozsah IP adres několika zařízení (například *192.168.0.1-192.168.0.99*).✓ **Podsít** – umožní zadat podsít skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsít 192.168.1.0. Chcete-li vyloučit celou podsít, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).**Podsít** – podsít skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Správa seznamu URL adres

Správa seznamu URL adres v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana přístupu na web** umožňuje zadat HTTP adresy, které se mají blokovat, povolit nebo vyloučit z kontroly obsahu webu.

Pokud chcete filtrovat kromě HTTP adres kontrolovat také HTTPS adresy, musí být zapnutý protokol [SSL/TLS](#). V opačném případě by byl zakázán pouze přístup na nešifrovanou HTTPS verzi webové stránky.

Webové stránky zařazené na **Seznamu blokových 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 blokových adres** * (hvězdičku).

V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Adresy vyloučené z kontroly se nekontrolují na přítomnost hrozeb, proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Je potřeba dbát opatrnosti při

používání speciálních znaků v tomto seznamu. Pro více informací, jak bezpečně přidat celou doménu včetně jejich subdomén, přejděte do kapitoly [Přidání masky adresy/domény](#). Pro aktivování seznamu vyberte možnost **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit zobrazení upozornění zaškrtnutím možnosti **Upozornit při aplikování adresy ze seznamu**.

Adresy důvěryhodné pro ESET

i Pokud je v nastavení [SSL/TLS](#) zapnuto **Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné**, domény na seznamu důvěryhodných adres spravovaném společností ESET nebudou ovlivněny konfigurací Správy seznamu URL adres.

Seznam adres

Název seznamu	Typy adres	Popis seznamu
Seznam povolených adres	Povolené	
Seznam blokováných adres	Blokované	
Seznam adres vyloučených z kontroly obsahu	Nalezený škodlivý kód je i...	

Přidat **Změnit** **Odstranit** **Importovat** **Exportovat**

Použitím zástupného znaku (*) v seznamu blokováných adres zablokujete všechny URL adresy kromě těch, které jsou definovány na seznamu povolených adres.

OK **Zrušit**

Ovládací prvky

Přidat – umožňuje vytvořit nový seznam. To je užitečné, pokud chcete adresy rozdělit do logických skupin. Například jeden seznam blokováných adres může obsahovat adresy z veřejných blacklistů, a druhý vámi definované adresy. V takovém případě je správa seznamu externích adres mnohem snadnější.

Změnit – kliknutím upravíte existující seznam adres. Tuto možnost použijte pro přidání nebo odebrání adres ze seznamu.

Odstranit – odebere existující seznam. Toto platí pouze na seznamy vytvořené ručně pomocí volby **Přidat**, nikoli předdefinované.

Seznam adres

V této části můžete zadat seznamy HTTP(S) adres, které budou blokovány, povoleny nebo vyloučeny z kontroly.

Standardně jsou k dispozici tři seznamy:

- **Seznam adres vyloučených z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na škodlivý kód.

- **Seznam povolených adres** – pokud do seznamu blokových 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 blokových adres.
- **Seznam blokových 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**.

Název seznamu	Typy adres	Popis seznamu
Seznam povolených adres	Povolené	
Seznam blokových adres	Blokované	
Seznam adres vyloučených z kontroly obsahu	Nalezený škodlivý kód je i...	

Použitím zástupného znaku (*) v seznamu blokových adres zablokuje všechny URL adresy kromě těch, které jsou definovány na seznamu povolených adres.

Názorné ukázky



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

- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Blokovat webovou stránku za použití produktů ESET pro domácnosti](#)

Další informace naleznete v části [Správa seznamu URL adres](#).

Vytvoření nového seznamu URL adres

V tomto dialogovém okně můžete vytvořit nový [seznam adres/masek](#), které budou blokovány, povoleny, nebo vyloučeny z kontroly.

Při vytváření nového seznamu jsou dostupné následující možnosti:

Typ seznamu adres – k dispozici jsou tři typy předdefinovaných seznamů:

- **Vyloučené z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na přítomnost škodlivého kódu.
- **Blokované** – na adresy v tomto seznamu nebude povolen přístup.
- **Povolené** – pokud do seznamu blokových 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 blokových 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 seznam například blokových nebo povolených stránek. V oznámení se zobrazí název seznamu obsahujícího zadanou webovou stránku.

Zaznamenávat od úrovně – informace o konkrétním seznamu používaném při přístupu na webové stránky lze zapisovat do [souborů protokolu](#).

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).

Jak přidat masku URL?

Před zadáním požadované masky adresy/domény se seznamte s instrukcemi.

ESET Smart Security Premium 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.).

Pokud použijete "*" na začátku názvu domény, bude sekvence vyhodnocena odlišně. Zprvu, zástupný znak hvězdičky ("*") v tomto případě nenahrazuje lomítko ("/"). To proto, aby se například maska *.domena.cz nevyhodnocovala jako adresa <http://jakakolidomena.cz/cesta#.domena.com> (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 *.domena.cz platí také pro adresu <http://domena.cz>. Použití masky *.domena.cz ovšem není správné, protože za daných okolností můžete být použita také pro adresu <http://jinadomena.cz>.

Kontrola HTTP(S) komunikace

Ve výchozím nastavení je aplikace ESET Smart Security Premium nakonfigurována tak, aby kontrolovala HTTP a HTTPS komunikaci, kterou používají internetové prohlížeče a další aplikace. Kontrolu komunikace byste měli zakázat pouze v případě, že máte problémy se softwarem třetí strany a chcete zjistit, zda tento problém způsobuje ESET Smart Security Premium.

Zapnout kontrolu HTTP komunikace – HTTP komunikace je vždy kontrolována na všech portech pro všechny aplikace.

Zapnout kontrolu HTTPS komunikace – HTTPS komunikace používá k přenosu informací mezi serverem a klientem šifrovaný kanál. ESET Smart Security Premium kontroluje komunikaci pomocí protokolů SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovat pouze komunikaci na portech definovaných v části **Porty používané protokolem HTTPS** bez ohledu na verzi operačního systému (k předdefinovaným portům 443 a 0-65535 můžete přidat další).

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

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

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web

- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochrany 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 schopnosti produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizacího 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 Smart Security Premium během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET Smart Security Premium

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.
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 doporučeno 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 určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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 ji 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](#) zapíše všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnutí Smart optimalizaci je použito neoptimálnější 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.

Rodičovská kontrola

Prostřednictvím možnosti **Zapnout rodičovskou kontrolu** se do prohlížečů integrují nastavení z [Rodičovské kontroly](#) ESET Smart Security Premium. Kliknutím na **Změnit** vedle položky [Uživatelské účty](#) můžete přiřadit uživatelské účty systému Windows používané Rodičovskou kontrolou ke konkrétním uživatelům a omezit jejich přístup k nevhodnému nebo škodlivému obsahu na internetu.

Uživatelské účty

V [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana přístupu na web** > **Rodičovská kontrola** > **Uživatelské účty** > **Změnit** můžete přiřadit uživatelské účty systému Windows používané Rodičovskou kontrolou konkrétním uživatelům a omezit jim tak přístup k nevhodnému nebo škodlivému obsahu na internetu.

Sloupce

Windows účet – název uživatelského účtu ve Windows.

Zapnuto – pomocí přepínače rozhodněte, zda má být rodičovská kontrola pro tento účet aktivní.

Název počítače – název počítače, případně domény, do které uživatel patří.

Datum narození – na základě definovaného data se vypočte věk dítěte, podle kterého se automaticky nastaví blokovací pravidla.

Ovládací prvky

Přidat – po kliknutí se zobrazí dialogové okno [Nastavení účtu](#).

Změnit – umožňuje upravovat vybrané účty.

Odstranit – odstraní vybraný uživatelský účet.

Aktualizovat – pokud jste přidali nový uživatelský účet, ale zatím se v seznamu nezobrazil, klikněte na toto tlačítko nebo znovu otevřete dialogové okno ESET Smart Security Premium.

Nastavení uživatelského účtu

Dialogové okno obsahuje tři záložky:

Obecné

Pomocí přepínače vedle **Zapnuto** aktivujte rodičovskou kontrolu pro níže zvolený Windows účet.

Klikněte na **Vybrat** pro vybrání některého ze uživatelských účtů v systému Windows ve vašem počítači. Mějte na paměti, že omezení přístupu na web se aplikuje pouze na uživatelský účet se standardním oprávněním. Uživatelé s administrátorským oprávněním si mohou nastavení kdykoli změnit.

Pokud se jedná o váš uživatelský účet, tedy rodiče, vyberte možnost, že se jedná o **účet rodiče**.

Na základě definovaného **data narození** se vypočte věk dítěte, podle kterého se automaticky nastaví blokovací pravidla pro přístup na webové stránky.

Zaznamenávat do protokolu

ESET Smart Security Premium ukládá důležité události do protokolu, který je možné prohlížet přímo v hlavním okně. Klikněte na **Nástroje > Protokoly** a z rozbalovacího menu **Protokolů** vyberte **Rodičovská kontrola**.

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů,
- **Informační** – zaznamenává informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy.
- **Varování** – do protokolu se zapíše kritické chyby a varovná hlášení.
- **Žádné** – nebudou zaznamenávány žádné události, nevytvoří se žádné protokoly.

Výjimky

Pomocí výjimek můžete jednotlivým uživatelským účtům definovat blokování nebo povolení přístupu na webové stránky, které nejsou v seznamu výjimek. Tato možnost je užitečná, když chcete blokovat pouze určité stránky, a ne celou kategorii. Výjimky vytvořené pro jeden účet lze zkopírovat a použít pro další. Pomůže vám to v případě, kdy vytváříte identická pravidla pro děti podobného věku.

Pro vytvoření nové výjimky klikněte na tlačítko **Přidat**. V zobrazeném dialogovém okně vyberte v rozbalovacím menu **Akci** (například **Blokovat**), zadejte **URL** adresu stránky a dokončete kliknutím na tlačítko **OK**. Výjimka se bude přidána na seznam existujících výjimek, včetně zobrazení stavu.

Přidat – kliknutím vytvoříte novou výjimku.

Změnit – po kliknutí můžete změnit parametry výjimky (**URL** a **akci**).

Odstranit – Odstranit vybranou výjimku.

Kopírovat – kliknutím na toto tlačítko můžete převzít seznam výjimek z jiného uživatelského účtu.

The screenshot shows a software window titled "Změnit uživatelský účet" (Change user account) from ESET SMART SECURITY PREMIUM. It has three tabs: "Obecné", "Výjimky" (selected), and "Kategorie". Under the "Výjimky" tab, there is a search bar and a table with two columns: "Akce" (Action) and "URL". The table is currently empty. Below the table are four buttons: "Přidat" (Add), "Změnit" (Change), "Odstranit" (Remove), and "Kopírovat" (Copy). To the right of these buttons are four arrow icons (up, down, left, right). At the bottom right of the dialog is a large "OK" button.

Výjimky definované v této záložce jsou nadřazeny definovaným kategoriím pro jednotlivé uživatelské účty. To znamená, že pokud je například pro určitý účet blokována kategorie **Zprávy**, ale zároveň je povolena výjimka pro URL stránku se zprávami, pak pro tento účet bude tato stránka přístupná. Změny provedené v tomto okně si můžete ověřit v sekci [Výjimky](#).

Kategorie

V této části můžete vybrat obecné **kategorie** webových stránek, které chcete danému uživateli blokovat nebo povolit. Použitím přepínače přístup na stránky z dané kategorie povolíte. Pokud ponecháte přepínač neaktivní, přístup na stránky z dané kategorie bude blokován.

Kopírovat – umožňuje zkopírovat seznam blokových nebo povolených kategorií z existujícího upraveného účtu.

SMART SECURITY PREMIUM

Změnit uživatelský účet

Obecné

Výjimky

Kategorie

Kategorie

Kategorie	Věk	Zapnuto
Agresivní	18+	<input checked="" type="checkbox"/>
Alkohol a tabákové výrobky	18+	<input checked="" type="checkbox"/>
Anonymizéry	18+	<input checked="" type="checkbox"/>
Automobilový průmysl	Kdokoli	<input checked="" type="checkbox"/>
Bez kategorie	18+	<input checked="" type="checkbox"/>
Cestování	Kdokoli	<input checked="" type="checkbox"/>
Chat a sociální sítě	12+	<input checked="" type="checkbox"/>

Kopírovat

OK

Kategorie

Ve sloupci **Zapnuto** označte políčka kategorií, které chcete povolit. Pokud ponecháte zaškrtnávací políčko prázdné, nebude kategorie pro daný účet povolena.

SMART SECURITY PREMIUM

Změnit uživatelský účet

Obecné

Výjimky

Kategorie

Kategorie

Kategorie	Věk	Zapnuto
Agresivní	18+	<input checked="" type="checkbox"/>
Alkohol a tabákové výrobky	18+	<input checked="" type="checkbox"/>
Anonymizéry	18+	<input checked="" type="checkbox"/>
Automobilový průmysl	Kdokoli	<input checked="" type="checkbox"/>
Bez kategorie	18+	<input checked="" type="checkbox"/>
Cestování	Kdokoli	<input checked="" type="checkbox"/>
Chat a sociální sítě	12+	<input checked="" type="checkbox"/>

Kopírovat

OK

Níže uvádíme příklady kategorií, jejichž obsah nemusí být na první pohled zřejmý:

- **Různé** – obvykle lokální adresy intranetu, 127.0.0.0/8, 192.168.0.0/16, atd. Pokud stránka vrací chybu 403 nebo 404, pak také patří do této kategorie.

- **Nerozhodnuto** – tato kategorie obsahuje stránky, o kterých nelze rozhodnout z důvodu neúspěšného připojení do databáze rodičovské kontroly.
- **Nezařazeno** – neznámé stránky nezařazené do databáze rodičovské kontroly.
- **Dynamické** – stránky, které vás přesměrovávají na jiné stránky.

Ochrana prohlížeče

Ochrana prohlížeče je další úroveň ochrany vašeho zabezpečení a soukromí, která chrání paměť prohlížeče před kontrolou jinými procesy, zvyšuje ochranu proti keyloggerům a zabraňuje vkládání jakýchkoli dat souvisejících s online platbami upravených malwarem ze schránky do zabezpečeného prohlížeče. Chcete-li nakonfigurovat ochranu prohlížeče, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana prohlížeče** a vyberte jednu z následujících možností konfigurace:

- [Zabezpečené bankovníctví a prohlížení webu](#)
- [Seznam povolených souborů v Ochráně prohlížeče](#)
- [Rámeček prohlížeče](#)

Zabezpečené bankovníctví a prohlížení webu

[Zabezpečené bankovníctví a prohlížení webu](#) můžete nakonfigurovat v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana prohlížeče** > **Zabezpečené bankovníctví a prohlížení webu**.

Zabezpečené bankovníctví a prohlížení webu


Zapnout Zabezpečené bankovníctví a prohlížení webu – je-li zapnuto Zabezpečené bankovníctví a prohlížení webu, všechny [podporované webové prohlížeče](#) se ve výchozím nastavení spustí v zabezpečeném režimu.

Ochrana prohlížeče

Zabezpečit všechny prohlížeče – ve výchozím stavu zapnuto; pakliže je tato možnost zapnutá, budou se všechny [podporované webové prohlížeče](#) spouštět v zabezpečeném režimu.

Režim instalace rozšíření – z rozbalovacího menu vyberte typ rozšíření, jehož instalaci chcete povolit v prohlížečích zabezpečených produktem ESET:

- **Základní rozšíření** – povolena budou pouze ta nejdůležitější rozšíření vyvinutá konkrétním výrobcem prohlížeče.
- **Všechna rozšíření** – dojde k povolení veškerých rozšíření podporovaných konkrétním prohlížečem.

 Změna nastavení režimu instalace rozšíření nemá vliv na již nainstalovaná rozšíření prohlížeče.

Zabezpečený prohlížeč

Rozšířená ochrana paměti – po aktivování této možnosti bude paměť zabezpečeného prohlížeče chráněna před inspekci jinými procesy.

Ochrana klávesnice – po zapnutí této možnosti budou veškeré informace zadané prostřednictvím klávesnice do zabezpečeného prohlížeče skryty před dalšími aplikacemi. Zlepšujeme tak ochranu před [keyloggery](#).

Ochrana schránky – pokud je tato funkce zapnutá, ESET Smart Security Premium zabrání vkládání jakýchkoli dat souvisejících s online platbami upravených malwarem ze schránky do zabezpečeného prohlížeče. Tím je zajištěna ochrana před případným změnám provedeným škodlivým softwarem.

Rámeček prohlížeče - umožňuje přizpůsobit zobrazení [rámečku prohlížeče](#) v chráněných prohlížečích.

Seznam povolených souborů v Ochráně prohlížeče – umožňuje spravovat položky přidané do Seznamu povolených v Ochráně prohlížeče.

Ochrana soukromí a zabezpečení v prohlížeči

Zapnout Ochranu soukromí a zabezpečení v prohlížeči – pokud je tato možnost vypnutá, rozšíření Ochrana soukromí a zabezpečení v prohlížeči bude odinstalováno ze všech podporovaných prohlížečů ve všech účtech Windows.

Zapnout oznámení o Ochráně soukromí a zabezpečení v prohlížeči – pokud je tato možnost zapnutá, ESET Smart Security Premium bude zobrazovat oznámení o Ochráně soukromí a zabezpečení v prohlížeči.

Kontrola skriptů prohlížeče

Zapnout rozšířenou kontrolu skriptů v prohlížeči – pokud je tato funkce povolena, antivirový skener bude kontrolovat všechny JavaScriptové programy spouštěné v internetových prohlížečích.

00

Správa zařízení

ESET Smart Security Premium automaticky kontroluje zařízení (CD/DVD/USB/atd). Můžete blokovat nebo upravovat rozšířené filtry nebo oprávnění a umožnit uživateli přístup k danému zařízení a práci s ním. Tuto funkci můžete použít v případě, že chcete uživatelům zabránit v připojování výměnných médií k počítači.

Podporovaná externí zařízení:

- Datové úložiště (HDD, USB výměnné jednotky),
- CD/DVD,
- USB tiskárna,
- FireWire úložiště,
- Zařízení Bluetooth,

- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port,
- Přenosná zařízení (zařízení napájená baterií, jako jsou přehrávače médií, chytré telefony, zařízení plug-and-play, atd.)
- Všechny typy zařízení.

Nastavení správy zařízení můžete upravit v [Rozšířených nastaveních](#) > **Ochrany** > **Správa zařízení**.

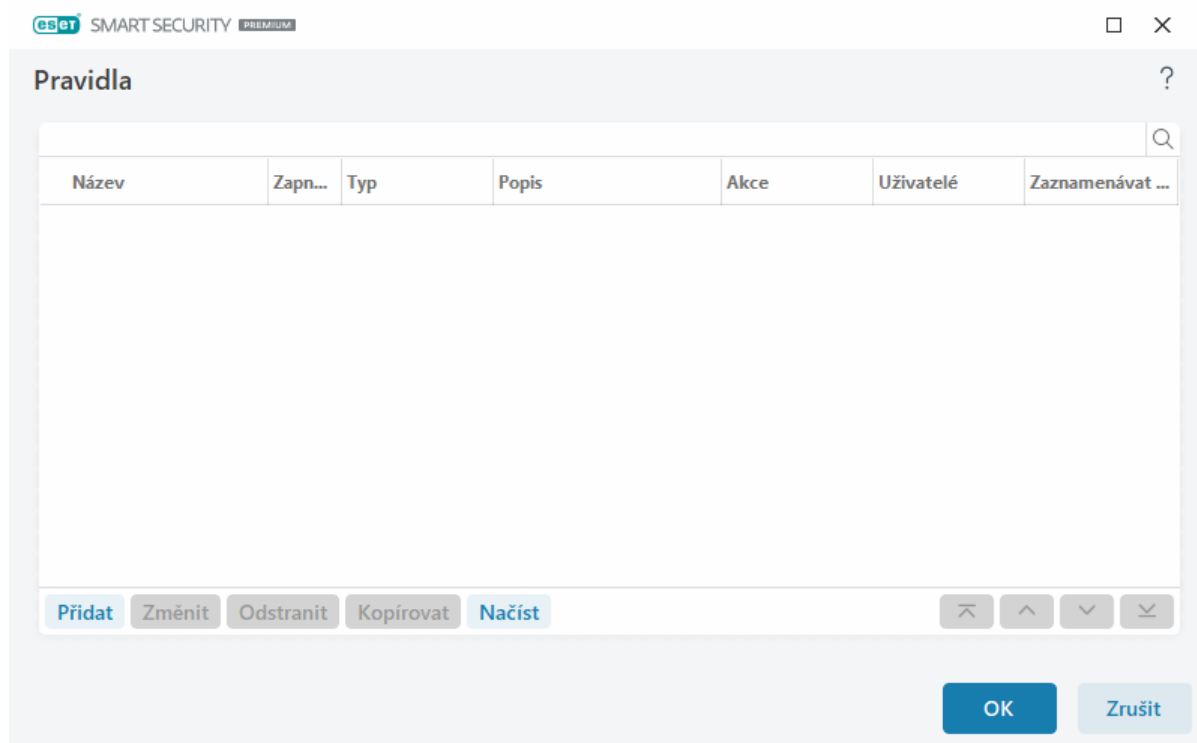
Přepínačem aktivujte **Povolit ovládání zařízení**, a povolte tak funkci Správa zařízení v ESET Smart Security Premium. Aby se tato změna projevila, musíte restartovat počítač. Po zapnutí správy zařízení se zpřístupní odkaz **Pravidla**, prostřednictvím kterého si otevřete [editor pravidel](#).

i Můžete vytvořit různé skupiny zařízení, na které se budou vztahovat různá pravidla. Vytvořte si skupinu zařízení, na kterou se bude aplikovat pravidlo pro **Povolení** nebo **Blokování zápisu**. Poté vytvořte druhé pravidlo, které bude blokovat přístup.

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.




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. Více si přečtete v kapitole [Pravidla správy zařízení](#).

Pro správu pravidel klikněte na tlačítko **Přidat** nebo **Změnit**. Kliknutím na tlačítko **Kopírovat** vytvoříte nové pravidlo s identickými parametry. XML řetězce zobrazené při kliknutí na pravidlo si můžete zkopírovat do schránky. To usnadní systémovým administrátorům export/import těchto dat a jejich opětovné použití.

Stisknutím klávesy **CTRL** a kliknutím můžete vybrat více pravidel najednou a provést hromadné akce, jako je jejich odstranění nebo posunutí dolů nebo vzhůru. **Zapnuto** – zaškrtnutím povolujete/zakazujete aplikaci pravidla. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

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**.


Záznamy protokolu lze zobrazit v [hlavním okně programu](#) > **Nástroje** > [Protokoly](#).

Do [protokolu správy zařízení](#) se zapisou informace o všech připojených zařízeních.

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). Pokud chcete zobrazit všechna skrytá zařízení, vyberte možnost **Zobrazit skrytá zařízení**.

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 varovnou ikonou . 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 probudte webovou kameru).

Vytvoření nového pravidla

V tomto okně můžete definovat akce, které se provedou po připojení daného zařízení k počítači.

eset SMART SECURITY PREMIUM

X

Přidat pravidlo?

Název

Bez názvu

Pravidlo je aktivní

☒

Typ zařízení

Datové úložiště

Akce

Povolit

Typ kritéria

Zařízení

Výrobce

Model

Sériové číslo

Zaznamenávat od úrovně

Vše

Seznam uživatelů

Změnit

Upozornit uživatele

☒

OK

Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla. Kliknutím na přepínač vedle **Pravidlo je aktivní** dané pravidlo zakázete nebo povolíte; to může být užitečné, pokud nechcete pravidlo trvale odstranit.

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.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

- **Povolit** – plný přístup k zařízení,
- **Blokovat** – přístup k zařízení bude zakázán,
- **Blokovat zápis** – uživatel může pouze číst soubory na daném zařízení, ale ne zapisovat.
- **Upozornit** – při každém připojení zařízení se uživateli zobrazí upozornění, že byl přístup na zařízení povolen/zakázán a zároveň se informace zapíše do protokolu. K zapamatování zařízení nedochází. Při opětovném připojení stejného zařízení dojde k zobrazení oznámení.

Mějte na paměti, že uvedené akce (povolení) nemusí být dostupné u všech zařízení. Pokud se jedná o úložné

zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

Typ kritéria

Vyberte, zda chcete pravidlo vytvořit pro jednotlivé **zařízení** nebo **skupinu zařízení**.

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.



Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.



Tip: Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a podívejte se do [protokolu správy zařízení](#).

Zaznamenávat do protokolu

ESET Smart Security Premium ukládá důležité události do protokolu, který je možné prohlížet přímo v hlavním okně. Protokoly naleznete v sekci **Nástroje > Protokoly** po vybrání možnosti **Správa zařízení** z rozbalovacího menu.

- **Vše** – zaznamenají se všechny události.
- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů,
- **Informační** – zaznamenány budou informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíše kritické chyby a varovná hlášení.
- **Žádné** – nebudou zaznamenávány žádné události, nevytvoří se žádné protokoly.

Seznam uživatelů

Pravidla přiřadíte konkrétnímu uživateli nebo celé skupině kliknutím na **Změnit** na řádku **Seznam uživatelů**.

- **Přidat** – otevře okno **Vybrat typ objektu: Uživatelé nebo Skupiny**, kde můžete vybrat konkrétní uživatele.
- **Odstranit** – odebere vybraného uživatele z filtru.

Omezení v seznamu uživatelů

Seznam uživatelů není možné definovat v pravidlech platných pro níže uvedené [Typy zařízení](#):



- USB tiskárna,
- Bluetooth zařízení,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port.

Upozornit uživatele – Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování a zobrazí se okno s oznámením.

Skupiny zařízení



Zařízení připojená k počítači mohou představovat bezpečnostní riziko.

Dialogové okno skupin zařízení je rozděleno na dvě části. V levé části se nachází seznam vytvořených skupin a v pravé části se zobrazují zařízení, která patří do dané skupiny. Pokud si chcete zobrazit v pravém okně zařízení, vyberte vlevo konkrétní skupinu zařízení.

Jakmile máte vybranou konkrétní skupinu, po kliknutí na příslušné tlačítko můžete zařízení do skupiny přidat nebo odstranit. Další možností přidání je import zařízení ze souboru. V neposlední řadě si kliknutím na tlačítko **Načíst** můžete zobrazit seznam všech zařízení připojených k počítači. Následně se vám zobrazí dialogové okno **Detekovaná zařízení**. Vyberte zařízení ze seznamu a přidejte je do skupiny kliknutím na tlačítko **OK**.

Ovládací prvky

Přidat – vytvoří novou skupinu nebo přidá zařízení do již existující skupiny, s ohledem na to, zda jste klikli na stejnojmenné tlačítko v levé nebo pravé části okna.

Změnit – umožňuje upravit název vybrané skupiny nebo parametry zařízení (výrobce, model, sériové číslo).

Odstranit – vymaže vybranou skupinu nebo konkrétní zařízení.

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

- Každé zařízení je uvedeno na samostatné řádce.
- **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).

Přidat zařízení

Kliknutím na tlačítko **Přidat** přidáte nové zařízení do existujícího seznamu zařízení. Pro přizpůsobení pravidel vztahených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.
- **Popis** – váš vlastní popis zařízení pro zjednodušení orientace v seznamu.

i Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.

Kliknutím na tlačítko **OK** uložíte změny. Klikněte na tlačítko **Zrušit** pro zavření dialogového okna **Skupiny zařízení** bez uložení změn.

i Po vytvoření skupiny zařízení je třeba pro ni [přidat nové pravidlo](#) a zvolit akci, která se má provést.

Mějte na paměti, že uvedené akce (povolení) nemusí být dostupné u všech zařízení. Pokud se jedná o úložiště, zobrazí se všechny možnosti. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

Ochrana webkamery

Ochrana webkamery vás informuje o procesech a aplikacích, které vyžadují přístup k webkameře. Pokud se aplikace pokusí o přístup, budete o tom informováni. V informačním okně můžete zvolit, zda chcete aplikaci **Blokovat přístup** nebo **Povolit přístup**. Barva okna závisí na úrovni rizika aplikace.

Nastavení ochrany webkamery lze upravit v [Rozšířených nastaveních](#) > **Ochrany** > **Správa zařízení** > **Ochrana webkamery**.

Ochranu webkamery v ESET Smart Security Premium aktivujete přepínačem vedle položky **Zapnout ochranu webkamery**.

Jakmile je Ochrana webkamery zapnutá, začnou se uplatňovat **Pravidla**. Kliknutím na odkaz **Změnit** můžete definovaná pravidla v [Editoru pravidel](#) měnit nebo odstranit.

Pokud chcete vypnout upozornění na aplikace s nastaveným pravidlem, které jste změnili, ale stále má platný digitální podpis (například po aktualizaci aplikace), zapněte kliknutím na přepínač možnost **Nezobrazovat upozornění týkající se přístupu ke kameře po změně aplikace**.

Editor pravidel ochrany webkamery

V tomto dialogovém okně naleznete pravidla, která aplikacím a procesům umožňují/zabraňují přistupovat k webkameře.

Dostupné jsou následující akce:

- **Povolit přístup**
- **Blokovat přístup**
- **Dotázat se** (zeptá se uživatele kdykoli při pokusu aplikace získat přístup k webkameře)

Pokud odškrtnete pole ve sloupci **Oznámit**, nebudou pokusy o přístup aplikací k webové kameře oznamovány.

Názorné ukázky



Pro podrobný popis nastavení v ESET Smart Security Premium si přečtěte článek v ESET Databázi znalostí [Jak vytvořit a upravit pravidlo v domácích produktech pro Windows \(10.x - 14.x\)](#) (článek nemusí být dostupný ve všech jazycích).

ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně, a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

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

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web

- Kontrola počítače

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime packerů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochrany 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 schopnosti produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizacího 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 Smart Security Premium během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET Smart Security Premium

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.
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 doporučeno 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 určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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 ji 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](#) zapíše 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 neoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena.

V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány.


Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik).

Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: **3 GB**.

 Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Úrovně léčení

Chcete-li změnit nastavení úrovně léčení pro určitý ochranný modul, rozbalte položku **ThreatSense** (například **Rezidentní ochrana souborového systému**) a poté z rozbalovacího menu vyberte **Úroveň léčení**.

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET Smart Security Premium

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.

Úroveň léčení	Popis
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučeno 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 určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Přípony souborů vyloučených z kontroly


Přípony vyloučených souborů jsou součástí [ThreatSense](#). Chcete-li nakonfigurovat přípony vyloučených souborů, klikněte na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli [modul, který používá technologii ThreatSense](#).


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

 Nezaměňujte tuto funkci s možností pro [vyloučení procesů](#), tvorbu [HIPS výjimek](#) nebo [vyloučení souborů/složek](#).

Standardně jsou kontrolovány všechny soubory. Do seznamu souborů vyloučených z kontroly můžete přidávat libovolné přípony.

Definovat výjimky je někdy nezbytné, jestliže jsou kontrolovány soubory s určitým rozšířením a kontrola by mohla mít negativní vliv na běh programu. Může být vhodné vyloučit např. `.edb`, `.eml` a `.tmp` pro MS Exchange Server).

 Pro přidání přípony klikněte na tlačítko **Přidat**. Do zobrazeného prázdného pole zadejte příponu (například `tmp`) a akci potvrďte kliknutím na tlačítko **OK**. Zadat můžete **více hodnot** oddělené čárkou, středníkem nebo zadejte každou příponu na nový řádek (například po vybrání možnosti **Středník** můžete zadat `edb ; eml ; tmp`).
Při definování seznamu výjimek můžete použít jako zástupný znak `?` (otazník). Otazník reprezentuje jeden znak (například `?db`).

 Chcete-li v operačním systému Windows zobrazit příponu souboru (pokud existuje), musíte zaškrtnout políčko **Přípony názvů souborů** v **Průzkumníku Windows > Zobrazit**.

Doplňující parametry ThreatSense

Chcete-li upravit tato nastavení, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Rezidentní ochrana souborového systému** > **Další parametry ThreatSense**.

Doplňující parametry ThreatSense pro nově vytvořený nebo upravený soubor

Pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s doplňujícími parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána rozšířená heuristika ESET Smart Security Premium, čímž se výrazně zvyšuje úroveň detekce, i když škodlivý kód ještě není znám před vydáním aktualizace detekčního jádra.

Kromě nově vytvářených souborů se kontrolují také **Samorozbalovací soubory** (.sfx) a **Runtime packery** (interně komprimované spustitelné soubory). Standardně jsou archivy kontrolovány do 10 úrovně vnoření bez ohledu na jejich velikost. Pro změnu nastavení kontroly archivů deaktivujte pomocí přepínače možnost **Standardní nastavení kontroly archivů**.

Doplňující parametry ThreatSense pro spouštěné soubory

Rozšířená heuristika pro spouštěné soubory – [rozšířená heuristika](#) se pro spouštěné soubory používá standardně. Pokud je zapnutá, důrazně doporučujeme ponechat zapnutou také [Smart optimalizaci](#) a [ESET LiveGrid®](#) pro snížení dopadu na výkon systému.

Rozšířená heuristika při spuštění souboru z výměnných médií – rozšířená heuristika emuluje kód aplikace ve virtuálním prostředí a vyhodnotí chování aplikace ještě předtím, než je povoleno aplikaci spuštění z výměnného média.

Nástroje

V [Rozšířených nastaveních](#) > **Nástroje** můžete nakonfigurovat pokročilá nastavení funkcí, které nabízejí dodatečné zabezpečení a pomáhají zjednodušit správu ESET Smart Security Premium.

- [Aktualizace operačního systému Windows](#)
- [ESET CMD](#)
- [Protokoly](#)
- [Herní režim](#)
- [Diagnostika](#)

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 nezbytné, abyste aktualizace systému Microsoft Windows instalovali, jakmile budou k dispozici. ESET Smart Security Premium vás upozorní na chybějící aktualizace podle úrovně, kterou jste zadali v [Rozšířených nastaveních](#) > **Nástroje**. 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.

Dialogové okno – Aktualizace systému

Pokud jsou připravené aktualizace pro váš operační systém, [hlavním okně programu](#) na záložce **Přehled** se zobrazí související oznámení. Po kliknutí na možnost **Více informací** se zobrazí dialogové okno s přehledem dostupných aktualizací.

V tomto dialogovém okně naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Řazený jsou dle názvu a vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Dvojklikem na konkrétní aktualizaci si zobrazíte podrobné [informace o dané aktualizaci](#).

Kliknutím na možnost **Spustit aktualizaci systému** stáhnete a nainstalujete všechny uvedené aktualizace operačního systému.

Informace o aktualizacích

V dialogovém okně Aktualizace systému naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Tlačítkem **Spustit aktualizace systému** zahájíte stahování a instalaci aktualizací operačního systému.

Po kliknutí pravým tlačítkem myši na danou aktualizaci a vybrání možnosti **Zobrazit informace** se zobrazí podrobné informace o aktualizaci.

ESET CMD

Jedná se o funkci, která povolí používání pokročilých ecmd příkazů. Díky tomu můžete exportovat a importovat nastavení prostřednictvím příkazového řádku (ecmd.exe). Až dosud bylo možné exportovat nastavení pomocí [GUI](#). Export konfigurace ESET Smart Security Premium můžete provést do souboru formátu *.xml*.

Po zapnutí funkce ESET CMD (v **Rozšířeném nastavení** v sekci **Nástroje > ESET CMD**) pomocí přepínače do polohy zapnuto si vyberte způsob ověření:

- **Žádný** – pokud vyberete tuto možnost, nebude vyžadováno ověření. Tuto možnost nedoporučujeme, protože představuje potenciální bezpečnostní riziko. V takovém případě totiž bude možné importovat nepodepsané konfigurace.
- **Heslo pro přístup do rozšířených 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 nastavenou ochranu heslem, heslo nesouhlasí nebo importovaný *.xml* soubor není podepsán.

Poté, co aktivujete funkci ESET CMD, můžete pro importování a exportování konfigurace produktu ESET Smart

Security Premium 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 je **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.

Konfiguraci z nainstalovaného produktu exportujete příkazem:

`ecmd /getcfg c:\config\settings.xml`

Konfiguraci do nainstalovaného produktu naimportujete příkazem:

`ecmd /setcfg c:\config\settings.xml`

i Pokročilé `ecmd` příkazy je možné používat pouze lokálně.

Jak podepsat `.xml`/konfigurační soubor:

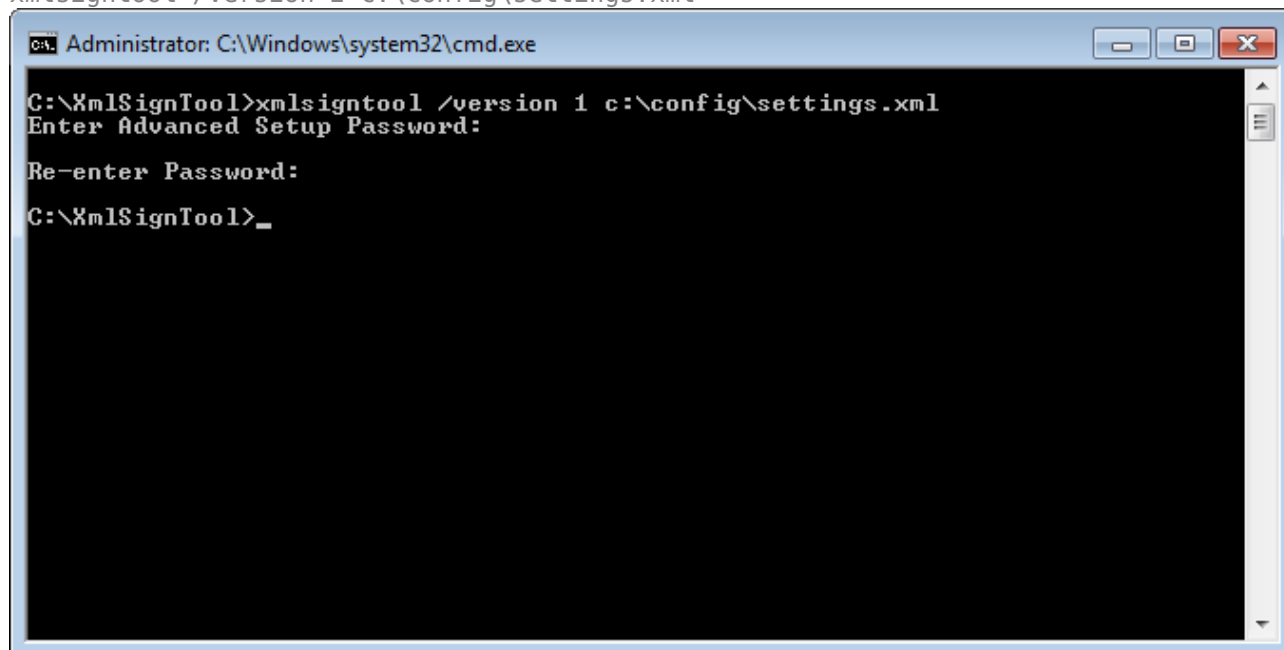
1. Z webových stránek společnosti ESET si stáhněte nástroj [XmlSignTool](#).
2. Příkazový řádek **Spustíte jako administrátor** (`cmd`).
3. Přejděte do složky se staženým nástrojem `xmlsigntool.exe`.
4. Konfigurační příkaz `.xml`/podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`

! Hodnota parametru `/version` závisí na verzi ESET Smart Security Premium. Pro verzi 11.1 a starší verze použijte `/version 1`. Pro ESET Smart Security Premium ve verzi 11.1 a novější použijte `/version 2`.

5. Na výzvu nástroje XmlSignTool zadejte a znovu zadejte [Heslo pro přístup do rozšířeného nastavení](#). Následně bude váš `.xml`/soubor s konfigurací programu podepsán a můžete jej prostřednictvím ESET CMD importovat do jiné instalace ESET Smart Security Premium.

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 .xm/souboru podepsaného původním heslem, podepište jej nejprve aktuálním heslem. To umožňuje použít dřívější konfigurační soubor bez nutnosti jej před importem exportovat z jiného zařízení se spuštěným ESET Smart Security Premium.



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 [rozšířených nastaveních](#) do sekce **Uživatelské rozhraní > Přístup k nastavení**.

Protokoly

Konfiguraci protokolování ESET Smart Security Premium najdete v [Rozšířených nastaveních](#) > **Nástroje** > **Protokoly**. V této sekci můžete upravit způsob správy protokolů. Program dokáže automaticky odstraňovat staré protokoly, čímž šetří místo na disku. V nastavení můžete vybrat následující možnosti:

Zaznamenávat události od úrovně – umožňuje nastavit úroveň, od které se budou zaznamenávat události do protokolu.

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



Všechna zablokovaná spojení se do protokolu zapíše 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 poli **Při překročení počtu nevyužitých záznamů (v procentech)**.

Kliknutím na **Optimalizovat** spustíte defragmentaci protokolů. Optimalizace 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 (pouze pro Text/CSV). Každá sekce protokolu má svůj vlastní soubor s předem definovaným názvem (například, virlog.txt pro sekci **Detekce** v souborech protokolů, pokud ukládáte protokoly ve formátu prostého textu).

- **Typ** – pokud vyberete **Text** jako formát souborů, protokoly budou uloženy do textového souboru, data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené čárkou **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.

i 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](#).

Herní režim

Herní režim je funkce navržená pro uživatele, kteří vyžadují nepřetržité používání softwaru, nechťejí být rušeni okny s oznámeními nebo upozorněními a chtějí minimalizovat používání CPU. Herní 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.

Herní režim můžete zapnout nebo vypnout v [hlavním okně programu](#) na záložce **Nastavení > Ochrana počítače** pomocí přepínače , resp.  na řádku **Herní režim**. Zapnutý herní 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 **Herní režim je zapnutý**.

Vybráním možnosti **Automaticky zapnout herní režim při zobrazení aplikací na celou obrazovku** se herní režim při takovém zobrazení automaticky zapne a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování herního režimu po spuštění hry nebo zahájení prezentace a najdete si v [Rozšířených nastaveních](#) (dostupném po stisknutí klávesy v hlavním okně programu) v sekci **Nástroje > Herní režim**.

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

i Pokud je firewall v Interaktivním režimu a zapnete Herní režim, mohou se vyskytnout problémy s připojením k internetu. Toto může představovat problém, například pokud spouštíte hru, která se k němu připojuje. Je to způsobeno tím, že za normálních okolností by si firewall vyžádal potvrzení připojení (pokud nejsou definována žádná pravidla nebo výjimky pro spojení), ale v Herním režimu jsou všechna vyskakovací okna vypnuta. Řešením je definovat pravidla nebo výjimky pro každou aplikaci, která by mohla mít konflikt s tímto chováním nebo použít jiný [Režim filtrování firewallu](#). Mějte také na paměti, že pokud při zapnutém Herním režimu pracujete s aplikací nebo stránkou, která představuje potenciální riziko, pak bude tato stránka zablokována, ale nezobrazí se žádné vysvětlení nebo varování, protože jsou vypnuty všechny akce vyžadující zásah uživatele.

Diagnostika

Diagnostika poskytuje výpisy ze selhání běhu procesů programu ESET (například ekrrn). Pokud aplikace spadne, vygeneruje se výpis, tzv. dump. Ten může pomoci vývojářům při ladění a opravě různých problémů v ESET Smart Security Premium.

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 marketingových zpráv – po zapnutí se budou zaznamenávat všechny události související s marketingovými zprávami, která se týkají produktu.

Aktivovat rozšířené protokolování antispamového jádra – po aktivování této možnosti se zaznamenají všechny události v průběhu kontroly zpráv. Toto nám pomůže diagnostikovat a odstranit potíže s antispamovým jádrem.

Aktivovat rozšířené protokolování technologie Anti-Theft – po aktivování této možnosti se zaznamenají všechny akce související s fungováním technologie Anti-Theft.

Aktivovat rozšířené protokolování Ochrany prohlížeče – po zapnutí se budou zaznamenávat všechny události, které se vyskytnou v zabezpečeném bankovníctví a prohlížení webu.

Aktivovat rozšířené protokolování skeneru – po zapnutí se do protokolu zaznamenají všechny události, které vznikly při volitelné kontrole počítače.

Aktivovat diagnostické protokolování správy zařízení – po aktivování této možnosti se do souboru zapíše 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 zapíše detailní informace z běhu ESET LiveGrid®. Toto pomůže vývojářům při diagnostice a řešení problémů s ESET LiveGrid®.

Aktivovat rozšířené protokolování ochrany dokumentů – po zapnutí se zaznamenají veškeré události související s modulem Ochrana dokumentů. Toto pomůže vývojářům při diagnostice a řešení problémů.

Aktivovat rozšířené protokolování ochrany poštovních klientů – po zapnutí se budou zaznamenávat všechny události, které se vyskytnou v Ochráně poštovních klientů a zásuvném modulu poštovního klienta, aby bylo možné diagnostikovat a řešit problémy.

Aktivovat rozšířené protokolování ESET LiveGuard – po zapnutí se zaznamenají všechny akce související s fungováním ESET LiveGuard.

Aktivovat rozšířené protokolování jádra – po zapnutí se zaznamenají všechny události, které se vyskytují v jádře ESET (ekrn).

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

Aktivovat výpis paměti – po zapnutí se budou zaznamenávat všechny události, které pomohou vývojářům při diagnostice úniku dat z paměti (memory leaku).

Aktivovat rozšířené protokolování síťové ochrany – po zapnutí se do souboru ve formátu PCAP bude zaznamenávat veškerá síťová komunikace vyhodnocovaná firewallem. Toto pomůže vývojářům při diagnostice a řešení problémů souvisejících firewallem.

Aktivovat rozšířené protokolování kontroly síťové komunikace – zaznamenávání všech dat procházejících kontrolou síťové komunikace do souboru ve formátu PCAP, který pomůže vývojářům při diagnostice a řešení problémů souvisejících s kontrolou síťového provozu.

Aktivovat rozšířené protokolování operačního systému – po aktivování se sesbírají dodatečné informace o operačním systému jako jsou běžící procesy, aktivita CPU a diskové operace. Toto pomůže vývojářům při diagnostice a řešení problémů s chodem programu ve vašem operačním systému.

Aktivovat rozšířené protokolování rodičovské kontroly – po aktivování této možnosti se do souboru zapíší detailní informace z běhu rodičovské kontroly. Toto nám pomůže diagnostikovat a odstranit potíže s rodičovskou kontrolou.

Aktivovat rozšířené protokolování push zpráv – po zapnutí se zaznamenají všechny události, ke kterým dojde během odesílání push zpráv.

Aktivovat rozšířené protokolování rezidentní ochrany souborového systému – po aktivování této možnosti se do protokolu zaznamenají všechny události, které vznikly při běhu rezidentní ochrany souborového systému.

Aktivovat rozšířené protokolování modulu aktualizace – po aktivování této možnosti se do souboru zapíší všechny události, ke kterým dojde během procesu aktualizace. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem zajišťujícím aktualizaci programu.

Protokoly se nachází ve složce `C:\ProgramData\ESET\ESET Security\Diagnostics\`.

Technická podpora

Pokud zakládáte z ESET Smart Security Premium požadavek na [Technickou podporu ESET](#), můžete zjednodušit práci našim expertům odesláním konfiguračních dat systému. Z rozbalovací nabídky **Odeslat konfiguraci systému** zvolte možnost **Odeslat vždy** pro automatické odeslání dat nebo **Dotázat se před odesláním**, pokud chcete mít před založením požadavku možnost volby.

Připojení

V určitých sítích může proxy server zprostředkovávat komunikaci mezi vaším zařízením a internetem. Pokud používáte proxy server, je třeba provést následující nastavení. V opačném případě se ESET Smart Security Premium a jeho moduly nemohou automaticky aktualizovat. V ESET Smart Security Premium je nastavení proxy serveru k dispozici ve dvou různých sekcích v [Rozšířených nastaveních](#).

V prvním případě můžete nastavení serveru konfigurovat v části [Rozšířená nastavení](#) > **Připojení** > **Proxy server**. Tato nastavení specifikují globální nastavení proxy serveru a tyto parametry se použijí pro jakýkoliv modul ESET Smart Security Premium. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

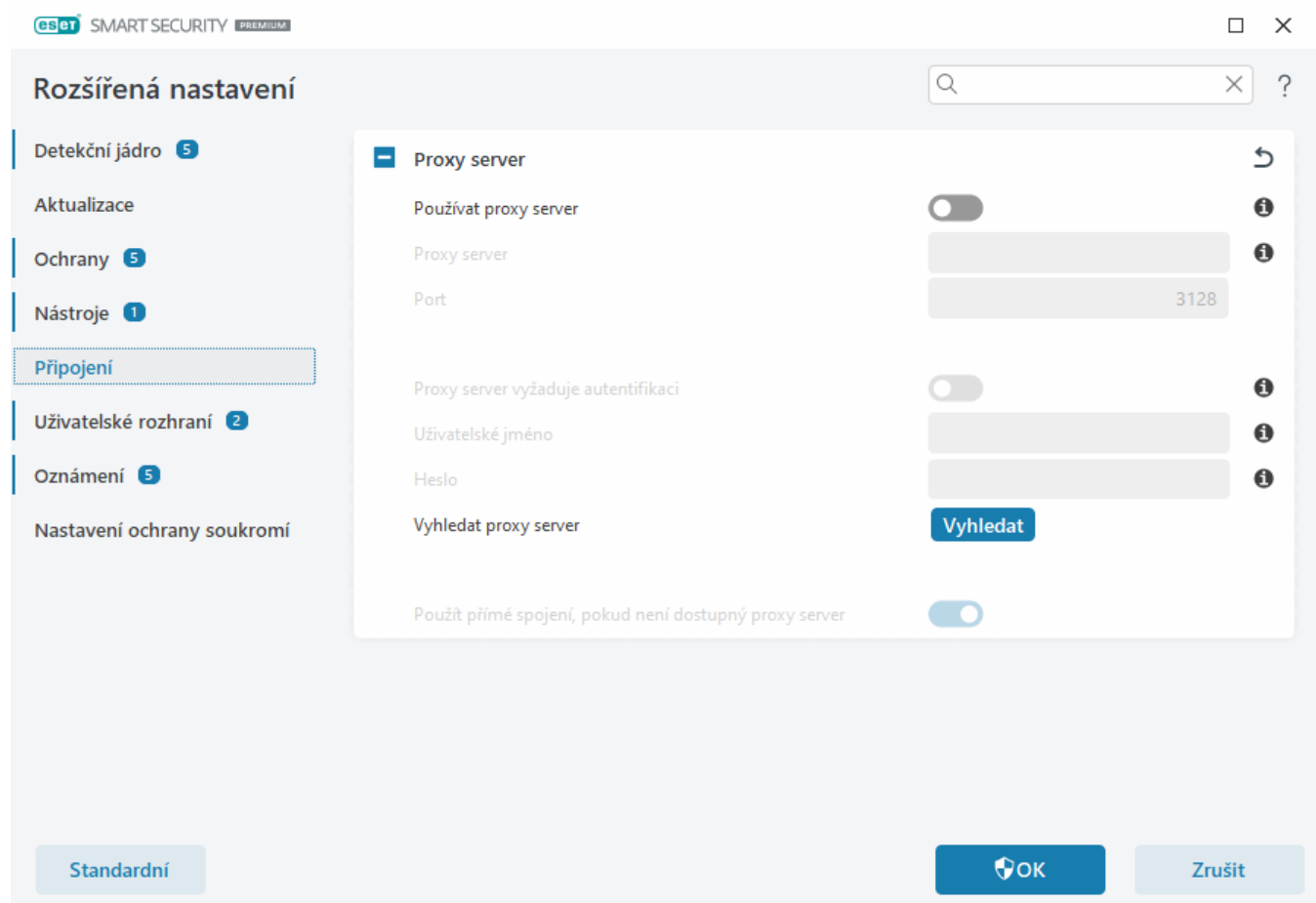
Chcete-li zadat globální nastavení proxy serveru, povolte možnost **Používat proxy server** a zadejte adresu **proxy serveru** spolu s číslem **portu** proxy serveru.

Pokud komunikace s proxy serverem vyžaduje ověření, vyberte možnost **Proxy server vyžaduje ověření** a do příslušných polí zadejte platné **uživatelské jméno** a **heslo**. Klepnutím na **Vyhledat proxy server** se automaticky zjistí a vyplní nastavení proxy serveru. ESET Smart Security Premium zkopíruje parametry zadané v možnostech internetu pro Internet Explorer nebo Google Chrome.

i V nastavení **proxy serveru** musíte ručně zadat své uživatelské jméno a heslo.

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

Nastavení proxy serveru lze provést také v [Rozšířených nastaveních](#) > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení** výběrem možnosti **Připojení prostřednictvím proxy serveru** v rozbalovací nabídce **Režim proxy**. Tato konfigurace platí pouze pro aktualizace a doporučuje se pro notebooky, které přijímají aktualizace modulů ze vzdálených umístění. Další informace naleznete v kapitole [Pokročilé nastavení aktualizace](#).



Uživatelské rozhraní

Chcete-li nakonfigurovat chování grafického uživatelského rozhraní (GUI) programu, otevřete [Rozšířená nastavení](#) > **Uživatelské rozhraní**.

V části [prvky uživatelského rozhraní](#) můžete přizpůsobit vzhled rozhraní a množství použitých efektů.

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu, stejně tak jeho odinstalaci, si v sekci [Přístup k nastavení](#) nastavte heslo.



Možnosti pro změnu chování systémových oznámení, upozornění na detekce a stavů aplikace naleznete v sekci [Oznámení](#).

Prvky uživatelského rozhraní

Uživatelské rozhraní ESET Smart Security Premium si můžete přizpůsobit svým potřebám. Tyto možnosti jsou dostupné v [Rozšířených nastaveních](#) v sekci **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

Barevný režim – v této části zvolte barevné schéma, ve kterém se bude uživatelské rozhraní ESET Smart Security Premium zobrazovat:

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



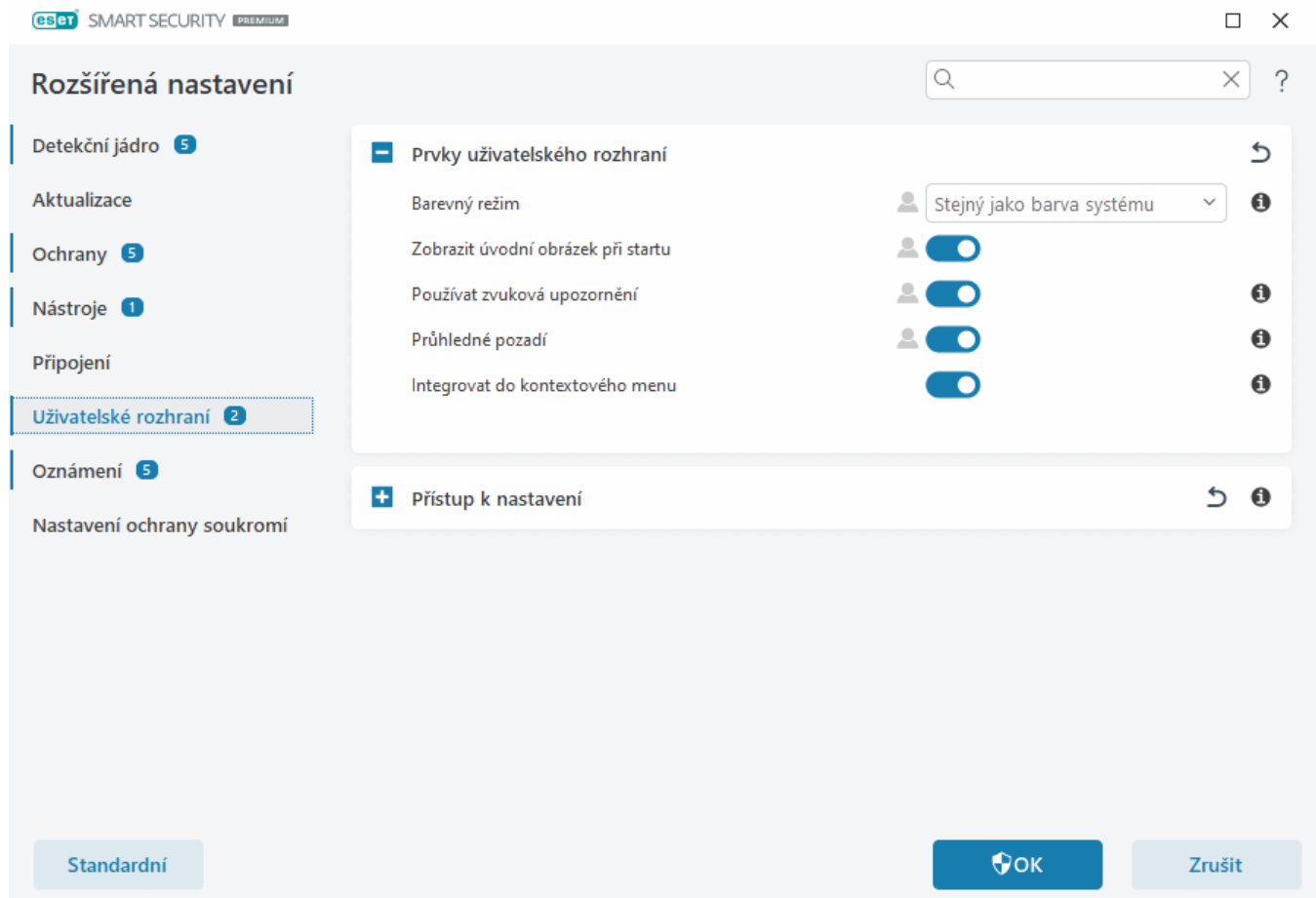
V pravém horním rohu [hlavního okna programu](#) si můžete navolit barevný režim, ve kterém se vám bude zobrazovat uživatelské rozhraní ESET Smart Security Premium.

Zobrazit úvodní obrázek při startu – po zapnutí se bude obrázek ESET Smart Security Premium zobrazovat na krátkou dobu po startu systému a následném prvním přihlášení k uživatelskému účtu Windows.

Používat zvuková upozornění – po zapnutí bude program přehrávat zvuky při důležitých událostech (například při detekci hrozby či dokončené kontrole)

Průhledné pozadí – pomocí této možnosti si zapnete efekt průhledného pozadí [hlavního okna programu](#). Průhledné pozadí je k dispozici pouze u nejnovější verze systému Windows (RS4 a novější).

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



Přístup k nastavení

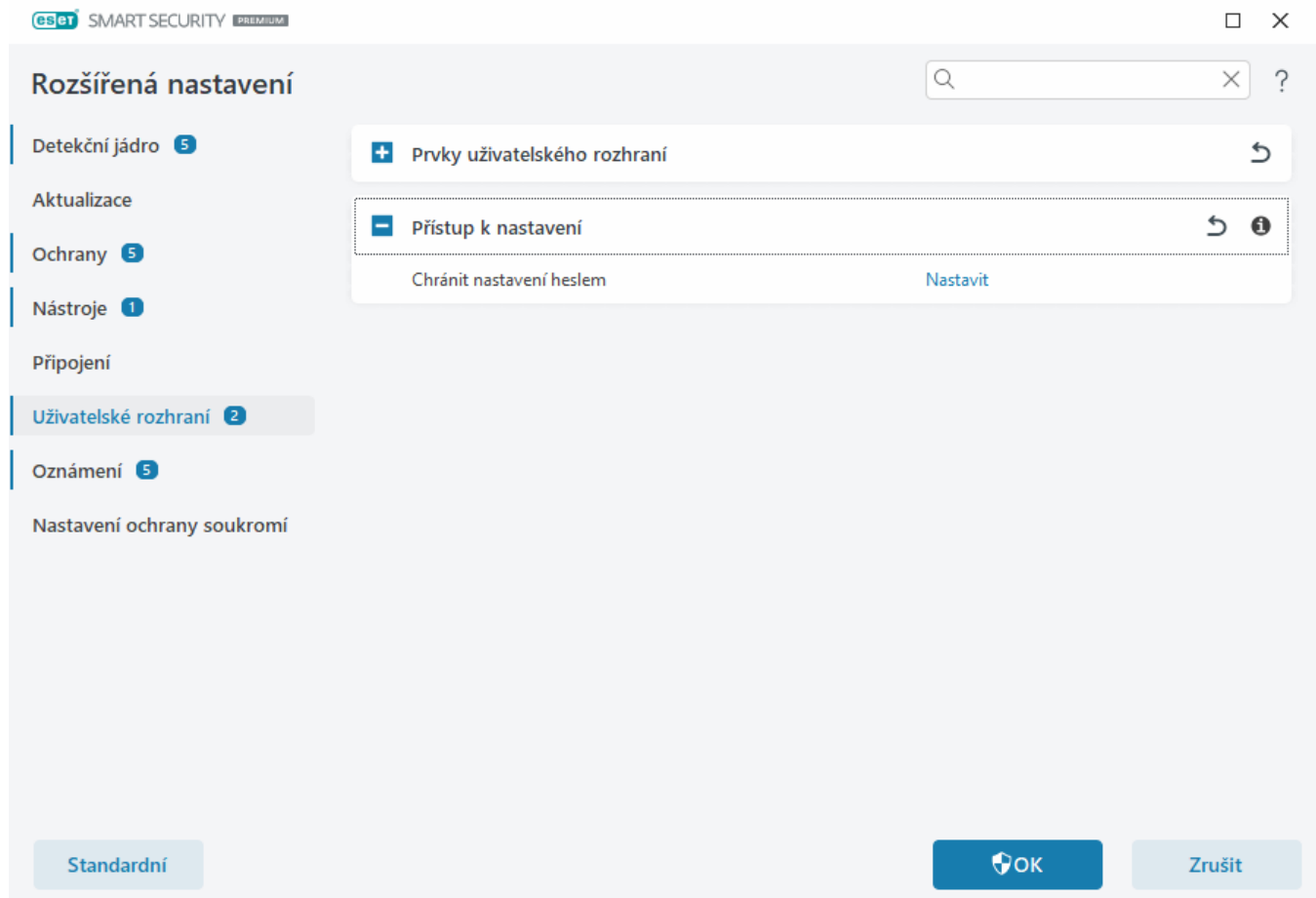
Správné nastavení ESET Smart Security Premium je velmi důležité pro celkové zabezpečení systému. Neoprávněná změna může vést ke snížení stability a ochrany. Prevencí proti neoprávněným změnám v ESET Smart Security Premium je možnost nastavení hesla. Nastavení přístupu lze konfigurovat v [Rozšířených nastaveních](#) > **Uživatelské rozhraní** > **Přístup k nastavení**.

Heslo jako prvek zabezpečení proti neoprávněnému nastavení ESET Smart Security Premium nebo odinstalaci nastavte, případně změňte kliknutím na **Nastavit** vedle položky **Chránit nastavení heslem**.

- i** Pokud chcete přejít do chráněného zobrazení Rozšířených nastavení, zobrazí se okno pro zadání hesla. Pokud zapomenete nebo ztratíte heslo, klikněte na **Obnovit heslo** níže a zadejte e-mailovou adresu, kterou jste použili při registraci předplatného. Na tuto adresu vám ESET zašle ověřovací kód společně s návodem na reset hesla.
- [Jak obnovit přístup do rozšířených nastavení?](#)

Pro změnu hesla klikněte na **Změnit heslo** vedle položky **Chránit nastavení heslem**.

Pro odstranění hesla klikněte na **Odstranit** vedle položky **Chránit nastavení heslem**.



Heslo pro přístup do Rozšířených nastavení

Rozšířená nastavení ESET Smart Security Premium doporučujeme ochránit před neoprávněnými změnami heslem. Heslo zadejte do polí **Nové heslo** a **Potvrzení hesla**. Klikněte na tlačítko **OK**.

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 k přístupu do Rozšířených nastavení.

Pokud heslo zapomenete, prostudujte si článek: [Co dělat, pokud zapomenete heslo do nastavení programu ESET](#)

Pro obnovení ztraceného aktivačního klíče ESET, data vypršení platnosti předplatného nebo dalších informací o předplatném pro ESET Smart Security Premium navštivte stránku [Ztratil jsem aktivační klíč](#).

Podpora odečítačů obrazovky

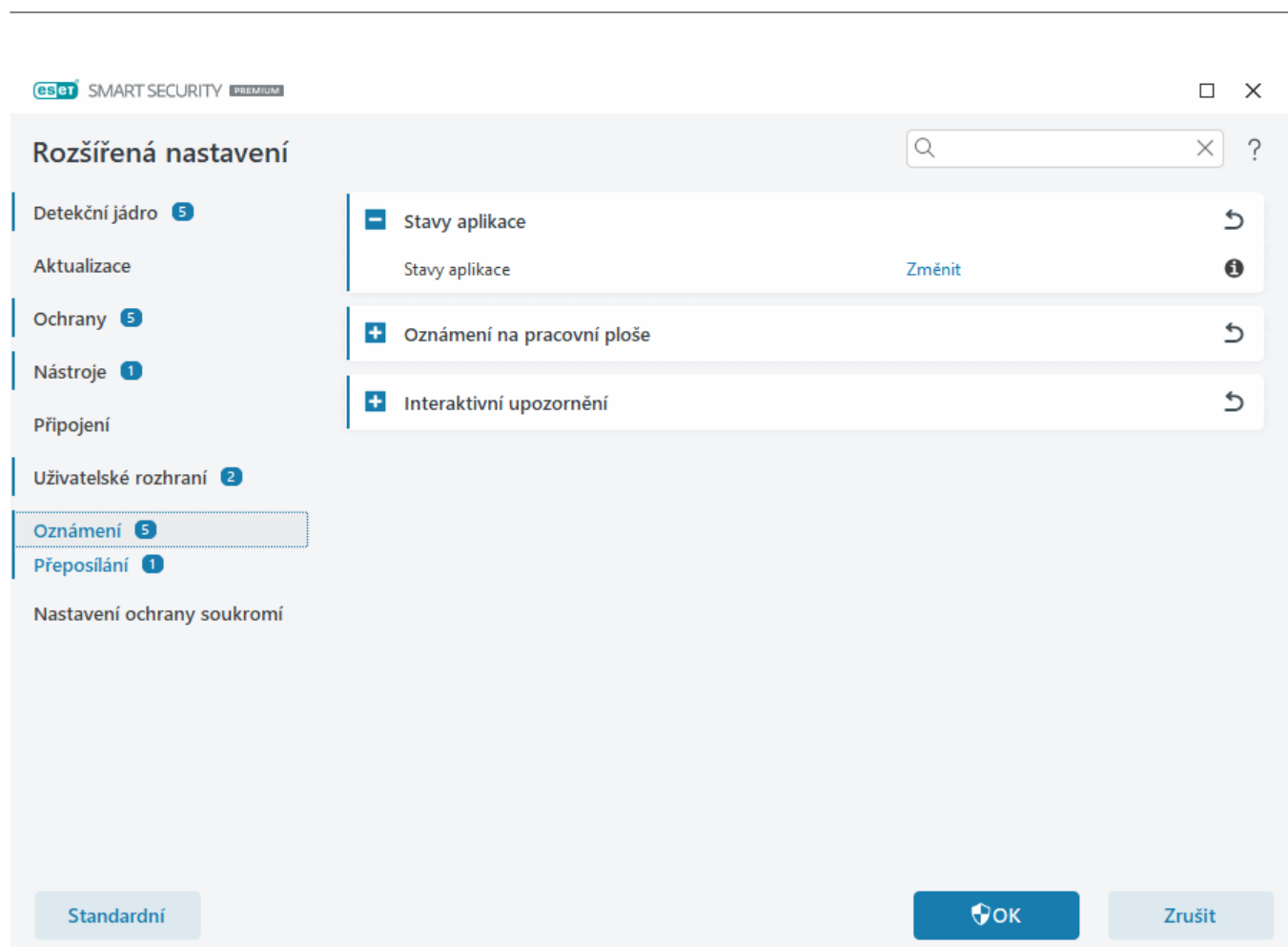
ESET Smart Security Premium lze použít společně s odečítači obrazovky, aby se mohli uživatelé ESET se zrakovým hendikepem lépe orientovat v produktu nebo konfigurovat nastavení. Podporovány jsou odečítače obrazovky (JAWS, NVDA, Narrator).

Pro kontrolu, zda má software odečítače obrazovky správný přístup k uživatelskému rozhraní ESET Smart Security Premium, si přečtěte návod v [Databázi znalostí](#).

Oznámení

Chcete-li spravovat oznámení ESET Smart Security Premium, otevřete [Rozšířená nastavení](#) > **Oznámení**. V této části můžete konfigurovat následující typy oznámení:

- Stavy aplikace – jedná se o oznámení, která se zobrazují v [hlavním okně programu](#) > **Přehled**.
- [Oznámení na pracovní ploše](#) – malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami).
- [Interaktivní upozornění](#) – výstražná upozornění a informační okna, která vyžadují interakci uživatele.
- [Přeposílání](#) (e-mailová oznámení) – oznámení se zasílají e-mailem na konkrétní adresy.



– Stavy aplikace

Stavy aplikace – po kliknutí na **Změnit** se můžete rozhodnout, jaké stavy aplikace chcete zobrazovat v [hlavním okně programu](#) > v části **Přehled**.

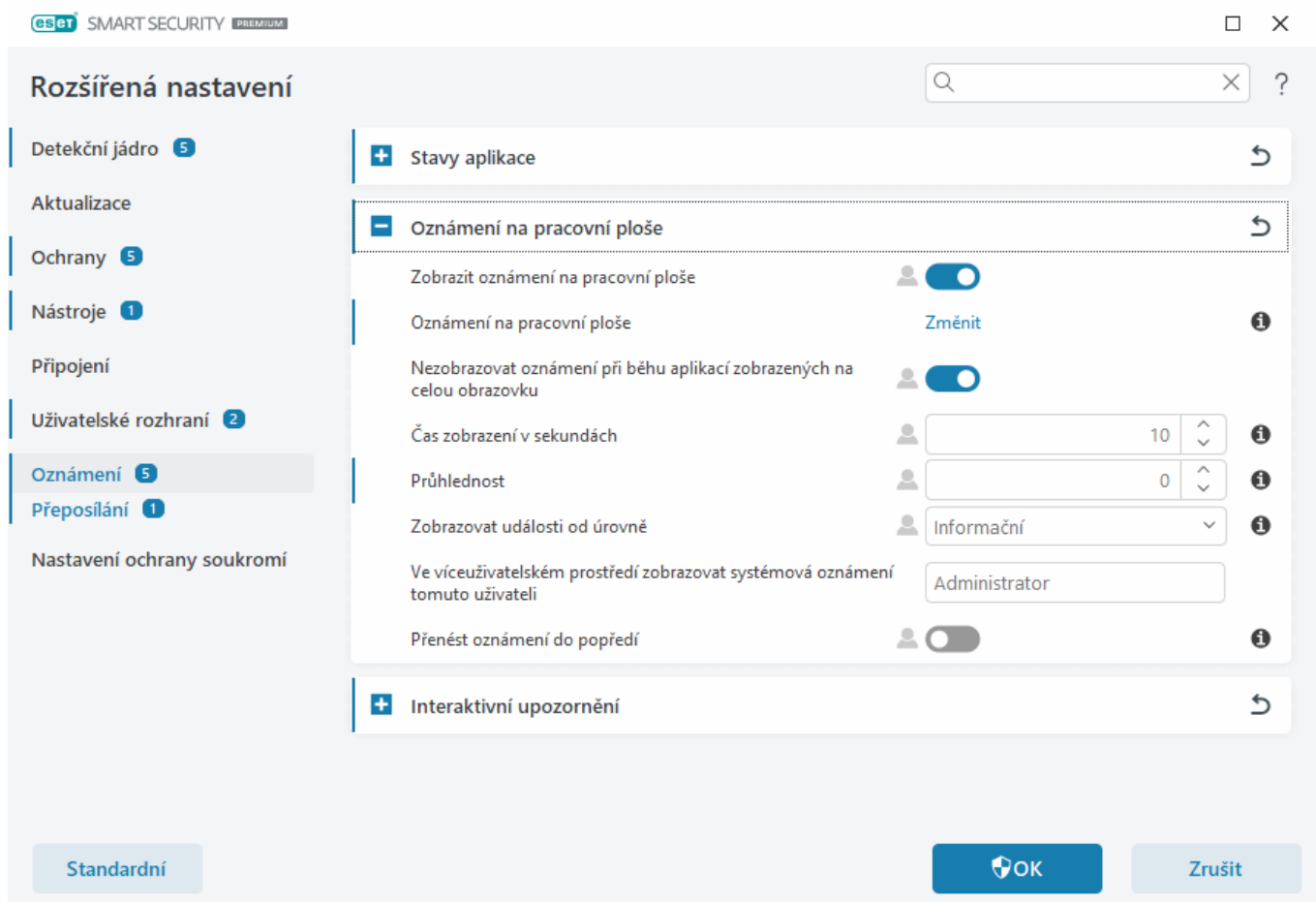
Dialogová okna – Stavy aplikace

V tomto dialogovém okně můžete aktivovat nebo deaktivovat upozornění na konkrétní stavy aplikace. Například můžete deaktivovat upozornění pro pozastavenou antivirovou a antispywarovou ochranu nebo zapnutý Herní režim.

Mezi sledované stavy aplikace patří také, zda je produkt aktivován nebo vypršela platnost vašeho předplatného.

Oznámení na pracovní ploše

Oznámení na pracovní ploše jsou malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami). Ve výchozím nastavení se zobrazí po dobu 10 sekund a následně pomalu zmizí. Oznámení zahrnují informace 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 zobrazení 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:

O Diagnostické – zobrazuje informace pro řešení problémů a všechny níže uvedené záznamy.

O Informativní – zobrazuje informativní zprávy o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy.

O Varování – zobrazuje varování, upozornění na chyby a kritické chyby (například, selhala aktualizace modulů).

O Chyby – zobrazuje chyby (například nefunkční ochrana dokumentů).

O Kritická – zobrazuje kritické chyby (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**.

Seznam oznámení na pracovní ploše

Kdykoli se můžete rozhodnout, jaká oznámení produktu chcete zobrazovat na pracovní ploše (v pravém dolním rohu obrazovky). Otevřete si [Rozšířená nastavení](#) > **Oznámení** > **Oznámení na pracovní ploše**. Na řádku **Oznámení na pracovní ploše** klikněte na **Změnit** a následně v zobrazeném dialogovém okně jednotlivá oznámení zapněte pomocí zaškrtnutí pole ve sloupci **Zobrazit na ploše**.

Vyberte oznámení, která chcete zobrazovat na pracovní ploše



Název	Zobrazit na ploše
AKTUALIZACE	
Detekční jádro bylo úspěšně aktualizováno	<input type="checkbox"/>
Je připravena aktualizace aplikace	<input checked="" type="checkbox"/>
Moduly byly úspěšně aktualizovány	<input type="checkbox"/>
OBEČNÉ	
Soubor byl odeslán k analýze	<input type="checkbox"/>
Zobrazit oznámení Co je nového	<input checked="" type="checkbox"/>
Zobrazovat oznámení z bezpečnostního přehledu	<input type="checkbox"/>
SÍŤOVÁ OCHRANA	
Upozornění na nezabezpečenou Wi-Fi	<input checked="" type="checkbox"/>

OK

Zrušit

Obecné

Zobrazovat oznámení z bezpečnostního přehledu - po zapnutí vás produkt upozorní na nově dostupný [bezpečnostní přehled](#).

Zobrazit oznámení Co je nového – vypnutím skryjete oznámení o všech nových a vylepšených funkcích nejnovější verze produktu.

Soubor byl odeslán k analýze – po jejím aktivování se zobrazí oznámení pokaždé, když produkt ESET Smart Security Premium zašlete soubor k analýze do virových laboratoří společnosti ESET.

Strážce sítě

Upozornit na nová zařízení připojená do vaší sítě – obdržíte oznámení, když je k síti připojeno nové zařízení.

Síťová ochrana

Profil sítě byl změněn – obdržíte oznámení o změně profilu sítě.

Upozornění na nezabezpečenou Wi-Fi – při pokusu o připojení k síti Wi-Fi se slabým nebo žádným heslem obdržíte upozornění.

Aktualizace

Je připravena aktualizace aplikace – po jejím aktivování budete upozorněni na dostupnou aktualizaci produktu ESET Smart Security Premium připravenou k nainstalování.

Detekční jádro bylo úspěšně aktualizováno – po zapnutí produkt zobrazí oznámení po každé aktualizaci detekčního jádra a programových modulů.

Moduly byly úspěšně aktualizovány – po zapnutí produkt zobrazí oznámení po každé aktualizaci programových komponent.

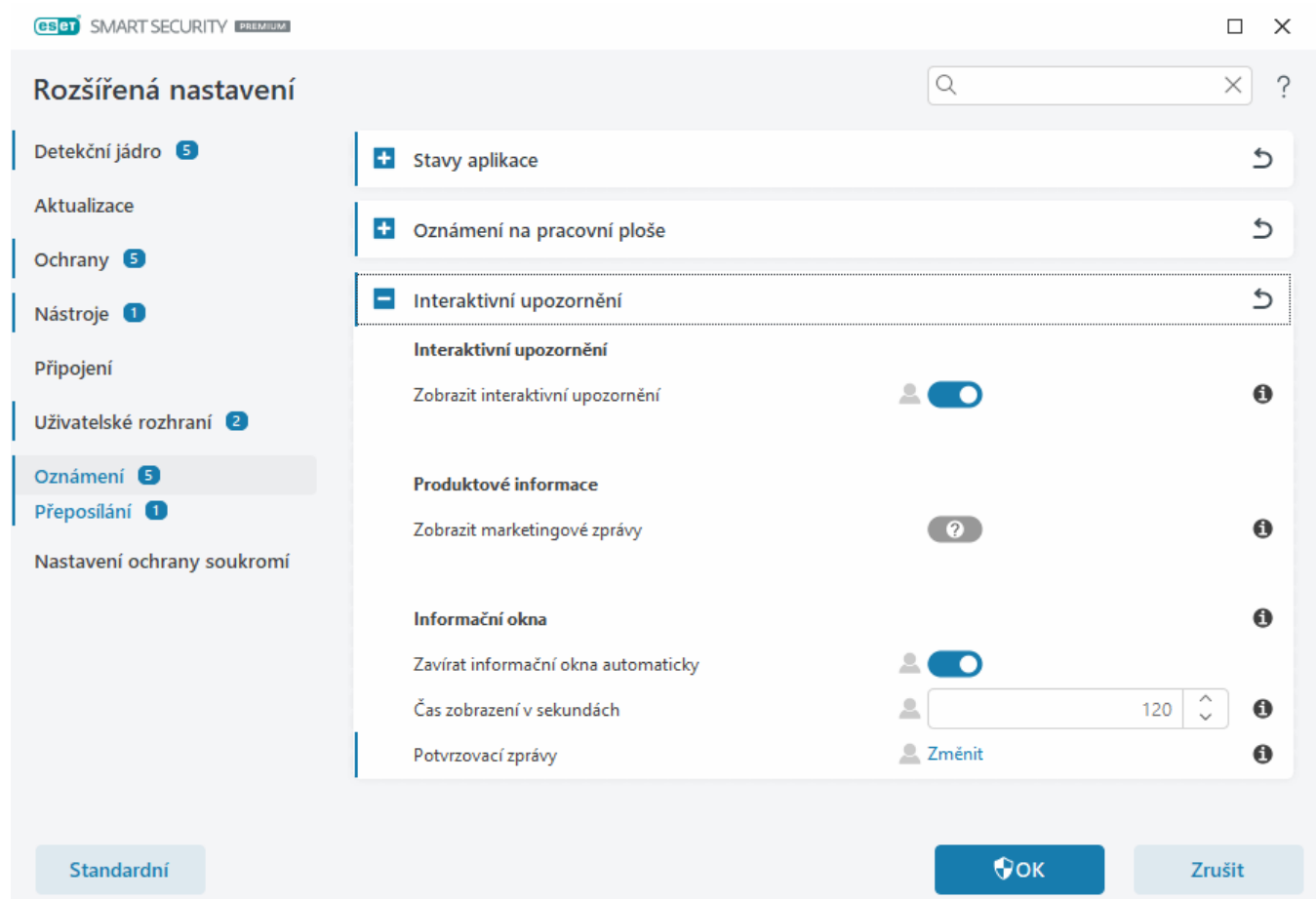
Obecná nastavení oznámení na ploše (například jak dlouho se má zpráva zobrazovat nebo minimální slovní rozsah zobrazovaných událostí) naleznete v části [Oznámení na ploše](#) v [Rozšířených nastaveních](#) > **Oznámení**.

Interaktivní upozornění

Hledáte informace o běžných upozorněních a oznámeních?

- [Nalezena hrozba](#)
- [Přístup na adresu byl zablokován](#)
- [Produkt není aktivován](#)
- [Změna na produkt s vyšším množstvím bezpečnostních funkcí](#)
- [Změna na produkt s nižším množstvím bezpečnostních funkcí](#)
- [Je dostupná aktualizace](#)
- [Informace o aktualizaci nejsou konzistentní](#)
- [Řešení problémů pro chybové hlášení "Moduly se nepodařilo aktualizovat"](#)
- [Řešení problémů s aktualizací modulů](#)
- [Zablokována síťová hrozba](#)
- [Certifikát webové stránky byl zamítnut](#)

V **Rozšířených nastaveních** v sekci [Oznámení](#) > **Interaktivní upozornění** můžete nastavit, jak se má ESET Smart Security Premium zachovat, pokud bude při detekci vyžadovat interakci uživatele (například při pokusu o přístup na potenciálně phishingovou stránku), stejně tak způsob zobrazování informačních oken.



Interaktivní upozornění

Vypnutí možnosti **Zobrazit interaktivní upozornění** skryje všechna dialogová okna s upozorněními, včetně informací ve webových prohlížečích. Tuto možnost je vhodné vypnout pouze v určitých situacích. Doporučujeme ponechat tuto možnost zapnutou.

Produktové informace

Zobrazení marketingových zpráv (tzv. in-product messaging) bylo navrženo pro informování uživatelů o novinkách a akcích společnosti ESET. Příjem marketingových zpráv vyžaduje váš souhlas. Ve výchozím stavu je u této položky zobrazena ikona otazníku a žádné zprávy nejsou zasílány. Zapnutím možnosti souhlasíte s jejich zasíláním. Pokud o sdělení nemáte zájem, pomocí přepínače na řádku **Zobrazit marketingové zprávy** možnost vypněte.

Informační okna

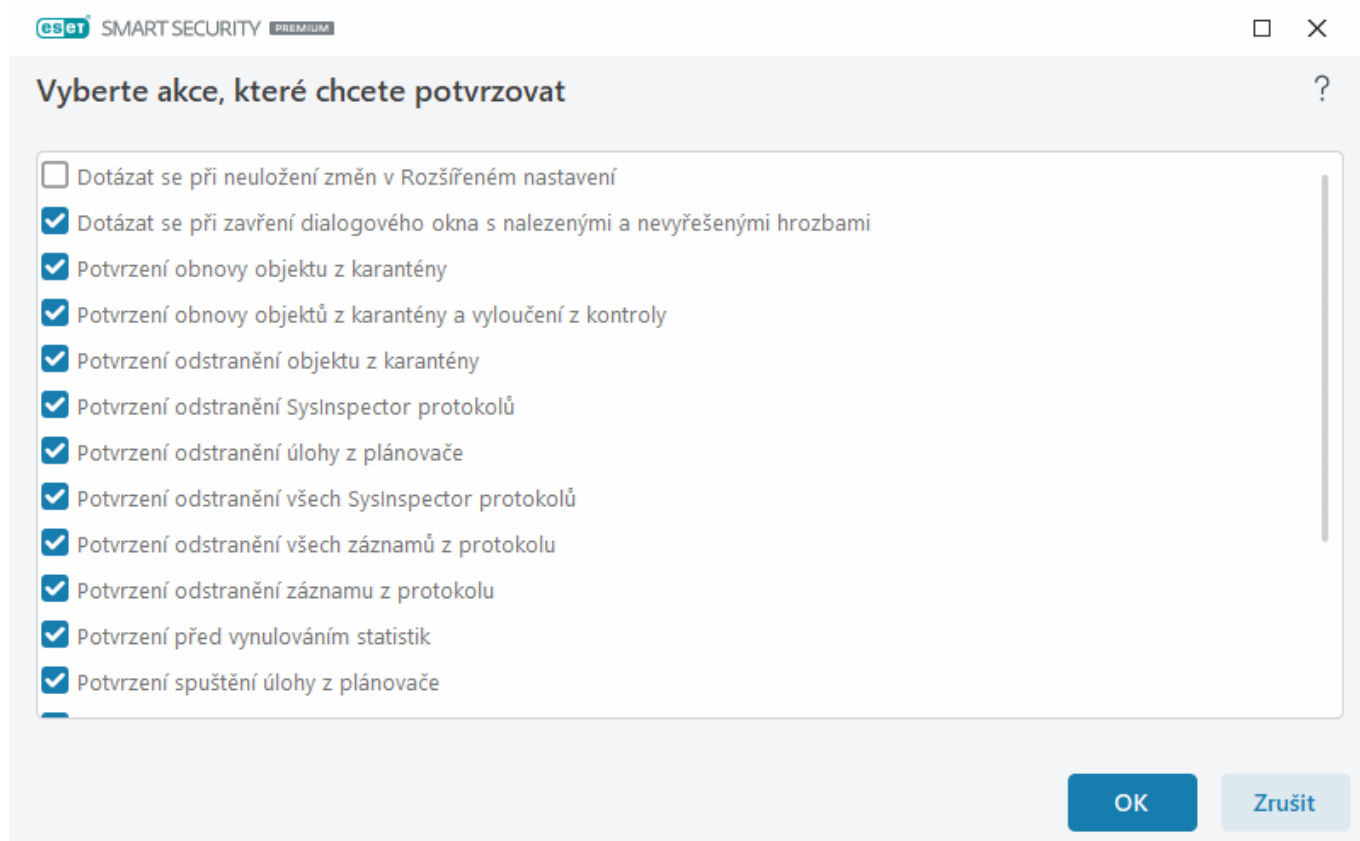
Dobu zobrazení informačních oken nastavíte pomocí možnosti **Zavírat informační okna automaticky**. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

Čas v sekundách – nastavuje dobu viditelnosti oznámení. Hodnota musí být mezi 10 a 999 sekundami.

Potvrzovací zprávy – pomocí této možnosti můžete spravovat [seznam potvrzovacích zpráv](#), jejichž zobrazování chcete povolit nebo zakázat.

Potvrzovací zprávy

Chcete-li upravit potvrzovací zprávy, otevřete [Rozšířená nastavení](#) > **Oznámení** > **Interaktivní upozornění** a klikněte na **Upravit** vedle položky **Potvrzovací zprávy**.



The screenshot shows a dialog box titled "Vyberte akce, které chcete potvrzovat" (Select actions you want to confirm) from ESET Smart Security Premium. The dialog has a title bar with the ESET logo, "SMART SECURITY PREMIUM", and window control buttons (minimize, maximize, close). A question mark icon is in the top right corner of the dialog area. The main content area contains a list of actions with checkboxes:

- ☐ Dotázat se při neuložení změn v Rozšířeném nastavení
- ☒ Dotázat se při zavření dialogového okna s nalezenými a nevyřešenými hrozbami
- ☒ Potvrzení obnovy objektu z karantény
- ☒ Potvrzení obnovy objektů z karantény a vyloučení z kontroly
- ☒ Potvrzení odstranění objektu z karantény
- ☒ Potvrzení odstranění SysInspector protokolů
- ☒ Potvrzení odstranění úlohy z plánovače
- ☒ Potvrzení odstranění všech SysInspector protokolů
- ☒ Potvrzení odstranění všech záznamů z protokolu
- ☒ Potvrzení odstranění záznamu z protokolu
- ☒ Potvrzení před vynulováním statistik
- ☒ Potvrzení spuštění úlohy z plánovače

At the bottom right, there are two buttons: "OK" and "Zrušit" (Cancel).

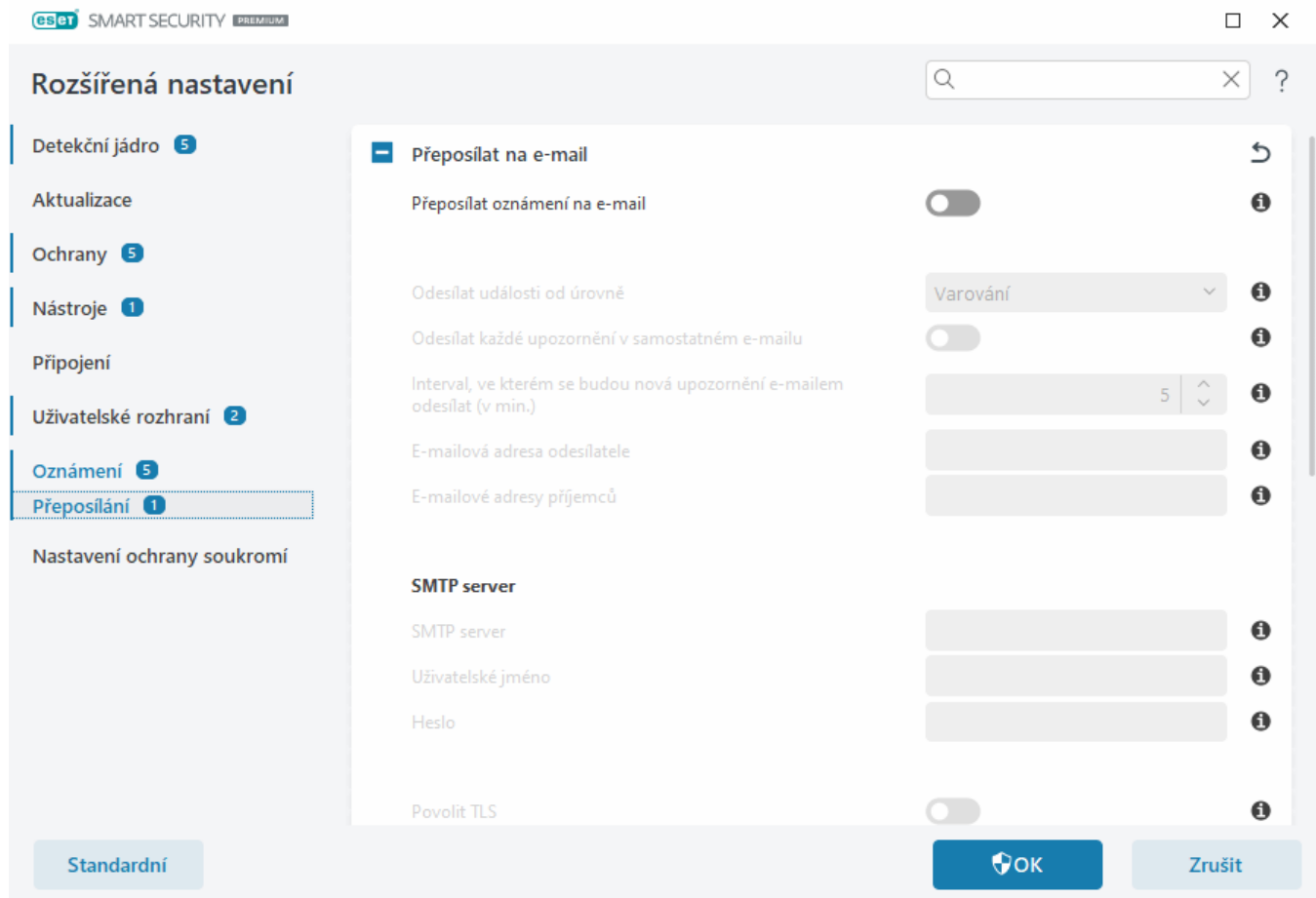
V tomto dialogovém okně můžete upravit zobrazování potvrzovacích zpráv, které ESET Smart Security Premium zobrazí před provedením akce. Pro jejich aktivaci nebo deaktivaci použijte zaškrtnávací pole na daném řádku.

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 Rozšířených nastaveních
- [Dotázat se při zavření dialogového okna s nalezenými a nevyřešenými hrozbami](#)
- [Potvrzení odstranění záznamu z protokolu](#)
- [Potvrzení odstranění úlohy z plánovače](#)
- [Potvrzení odstranění všech záznamů z protokolu](#)
- [Potvrzení před vynulováním statistik](#)
- [Potvrzení obnovení objektu z karantény](#)
- [Potvrzení obnovení objektů z karantény a vyloučení z kontroly](#)
- [Potvrzení spuštění úlohy z plánovače](#)
- [Zobrazit výsledek antispamové kontroly](#)
- [Zobrazit oznámení o výsledku antispamové kontroly provedené v poštovním klientovi](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovních klientů Outlook Express a Windows Mail](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Windows Mail](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Microsoft Outlook](#)

Přeposílání

ESET Smart Security Premium dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pro aktivování zaslání upozornění e-mailem otevřete [Rozšířená nastavení](#) > **Oznámení** > **Přeposílání** a zapněte možnost **Přeposílat oznámení na e-mail**.



Odesílat události od úrovně – specifikuje, od které úrovně důležitosti se budou upozornění na události odesílat.

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy,
- **Varování** – do protokolu se zapíše kritické chyby, chybová a varovná hlášení (například, aktualizace se nezdařila).
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například nefunkční ochrana dokumentů),
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany nebo infiltraci v systému),

Odesílat každé upozornění v samostatném e-mailu – pokud je tato možnost aktivní, příjemce obdrží při výskytu události nové upozornění. Při výskytu velkého množství událostí v krátkém čase obdrží příjemce velké množství e-mailů.

Interval, ve kterém se budou nová upozornění odesílat (v min.) – interval v minutách, po jehož uplynutí bude odeslán souhrnný e-mail se všemi upozorněními na události, které se v daném intervalu vyskytly. Pokud nastavíte hodnotu na 0, upozornění bude odesláno okamžitě po jeho výskytu.

E-mailová adresa odesílatele – specifikuje adresu odesílatele, která se použije v hlavičce e-mailové zprávy.

E-mailová adresa příjemce – specifikuje adresu příjemce, která se použije v hlavičce e-mailové zprávy. Podporováno je více hodnot. Jako oddělovač použijte středník.

SMTP server

SMTP server – adresa SMTP serveru, prostřednictvím kterého budou zprávy odesílány (například smtp.provider.com:587. Pokud nespecifikujete port, použije se výchozí 25).

 ESET Smart Security Premium podporují SMTP servery s TLS šifrováním.

Uživatelské jméno a heslo – v případě, že SMTP server vyžaduje autorizaci, musíte vyplnit tato pole pro přístup k SMTP.

Povolit TLS – po aktivování této možnosti se budou oznámení a bezpečnostní upozornění zasílat šifrovaně prostřednictvím TLS.

Otestovat konfiguraci SMTP – Pomocí tohoto tlačítka odešlete testovací e-mail na e-mailovou adresu příjemce. Je třeba, abyste před odesláním vyplnili údaje, jako SMTP server, uživatelské jméno, heslo, adresa odesílatele a adresa příjemce.

Formát zprávy

Komunikace mezi programem a vzdáleným uživatelem nebo systémovým administrátorem probíhá prostřednictvím e-mailu nebo LAN zpráv (s využitím služby Windows messaging). Standardně je aktivní možnost **Použít výchozí formát zprávy**, který je vhodný pro většinu situací. 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 otázníkem ("?").

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).

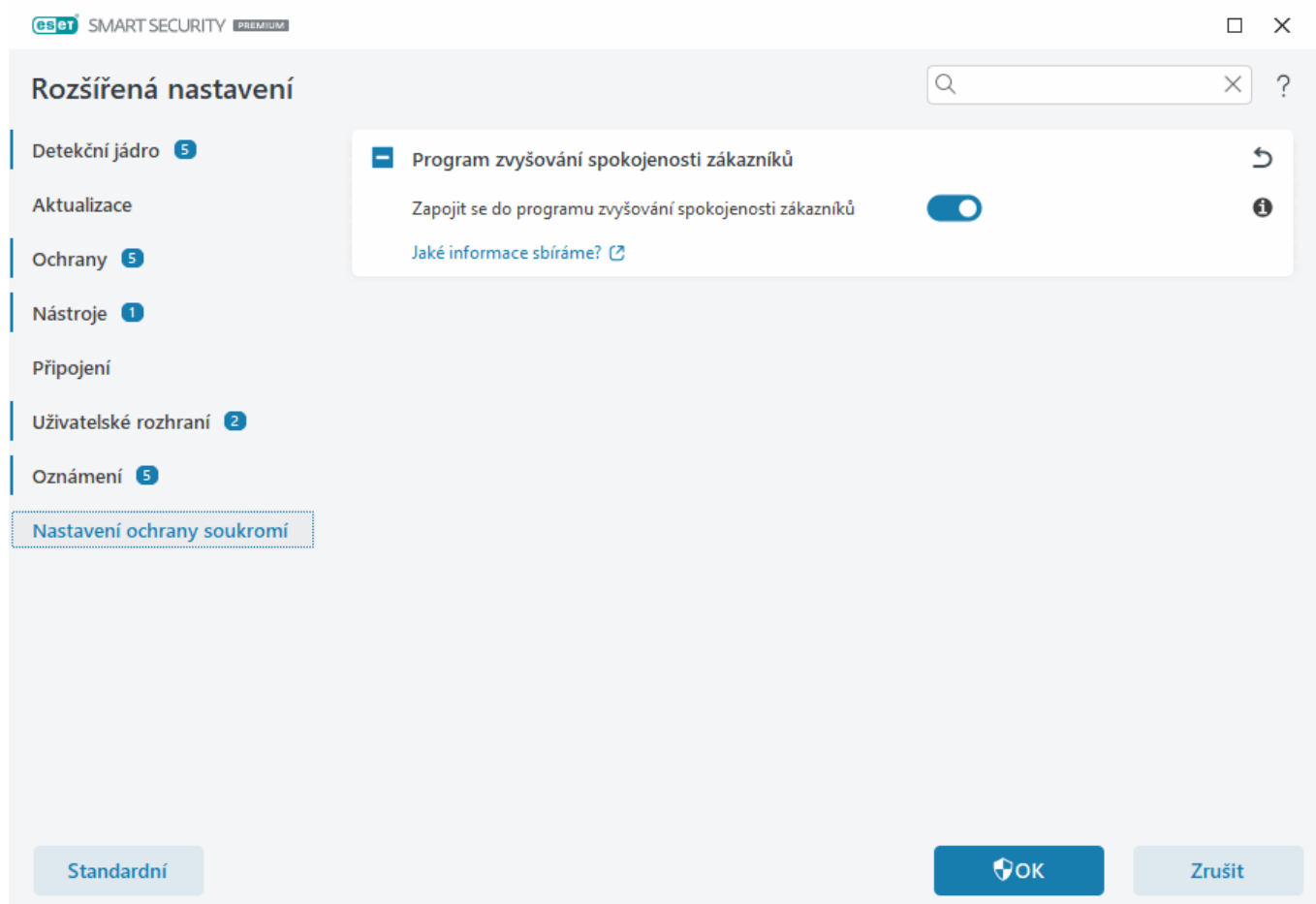
- **%TimeStamp%** – datum a čas události,
- **%Scanner%** – modul, který zaznamenal událost,
- **%ComputerName%** – název počítače, na kterém došlo k události,
- **%ProgramName%** – program, který způsobil událost,
- **%InfectedObject%** – název škodlivého souboru, e-mailové zprávy, apod.,

- **%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.

Nastavení ochrany soukromí

Otevřete [Rozšířená nastavení](#) > **Nastavení soukromí**.



Program zvyšování spokojenosti zákazníků

Aktivací pomocí přepínače se můžete **Zapojit do programu zvyšování spokojenosti zákazníků**. Zapojením do programu poskytnete společnosti ESET anonymní informace související s používáním našich produktů. Shromážděné údaje nám pomohou zlepšit produkty. Informace nebudou sdíleny se třetími stranami. [Jaké informace sbíráme?](#)

Obnovit všechna nastavení na standardní

Kliknutím na **Standardní** v [Rozšířených nastaveních](#) vrátíte zpět všechna nastavení aplikace pro všechny moduly. Tím zajistíte, že se nastavení vrátí do stavu, v jakém byla po nové instalaci.

Dále se můžete podívat do kapitoly [Import a export nastavení](#).

Obnovit všechna nastavení v této sekci na standardní

Kliknutím na ikonu šipky ↩ obnovíte všechna nastavení v dané sekci na výchozí hodnoty definované společností ESET.

Prosím, mějte na paměti, že po kliknutí na tlačítko **Obnovit na standardní** budou všechny dosavadní změny ztraceny.

Obnovit obsah tabulek – po aktivování této možnosti se odstraní všechna ručně i automaticky přidaná pravidla, úlohy i profily.

Dále se můžete podívat do kapitoly [Import a export nastavení](#).

Chyba během ukládání nastavení

Tato chyba značí, že nastavení nebylo správně uloženo z důvodu chyby.

To obvykle znamená, že uživatel, který se pokoušel modifikovat nastavení programu:

- nemá dostatečná přístupová oprávnění nebo nemá nezbytná oprávnění operačního systému pro úpravu konfiguračních souborů a záznamů v registru systému.
> Pro provedení požadovaných změn se musí přihlásit administrátor systému.
- aktivoval učicí režim modulu HIPS nebo firewallu, a pokouší se provádět změny v jejich nastavení.
> Pro uložení nastavení a zabránění konfliktu ukončete Rozšířená nastavení bez uložení změn, a zkuste změny provést znovu.

Druhou nejčastější příčinou bývá nekonzistentnost produktu, který nepracuje správně z důvodu svého poškození, a proto je nutné jej přeinstalovat.

Skener příkazového řádku

Modul antivirové ochrany produktu ESET Smart Security Premium 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 lze použít následující parametry a přepínače:

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=ÚROVNĚ	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 přidávají 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=ÚROVNĚ	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	vyločit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=REŽIM	<p>použít REŽIM léčení infikovaných objektů</p> <p>K dispozici jsou následující možnosti:</p> <ul style="list-style-type: none"> • 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 dotázáni 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.

FAQ

V této kapitole naleznete vybrané nejčastěji se vyskytující otázky a problémů, se kterými se můžete setkat. Klikněte na název kapitoly pro zobrazení řešení problému.

- [Jak aktualizovat ESET Smart Security Premium?](#)
- [ESET Smart Security Premium detekoval hrozbu](#)
- [Jak odstranit virus z počítače](#)
- [Jak povolit komunikaci pro konkrétní aplikaci?](#)
- [Jak zapnout rodičovskou kontrolu?](#)
- [Jak vytvořit novou úlohu v Plánovači?](#)
- [Jak naplánovat kontrolu \(týdně\)?](#)
- [Jak obnovit přístup do rozšířených nastavení?](#)
- [Jak deaktivovat produkt prostřednictvím portálu ESET HOME?](#)

Pokud není váš problém uveden v seznamu výše, zkuste v nápovědě k produktu ESET Smart Security Premium vyhledat řešení podle klíčového slova nebo fráze, která popisuje váš problém.

Pokud nenaleznete řešení vašeho problému v nápovědě k produktu ESET Smart Security Premium, navštivte pravidelně aktualizovanou [Databázi znalostí](#). Níže naleznete odkazy na nejnavštěvovanější články v Databázi znalostí:

- [Jak obnovit předplatné?](#)
- [Při aktivaci produktu ESET došlo k chybě. Co to znamená?](#)
- [Aktivace bezpečnostního produktu ESET pro Windows určeného pro domácnosti pomocí aktivačního klíče](#)
- [Jak odinstalovat nebo přinstalovat program ESET?](#)
- [Instalace programu ESET skončila předčasně](#)
- [Co musím udělat po obnovení předplatného? \(Domácí uživatelé\)](#)
- [Co se stane, pokud změním e-mailovou adresu?](#)
- [Jak mohu přenést produkt ESET do nového počítače?](#)
- [Jak spustit Windows v Nouzovém režimu nebo Nouzovém režimu se sítí](#)
- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Povolit odečítačům obrazovky přístup k uživatelskému rozhraní produktu ESET](#)

Pokud je to nutné, můžete se obrátit přímo na naše pracovníky [technické podpory](#).

Jak aktualizovat ESET Smart Security Premium?

Aktualizaci produktu ESET Smart Security Premium můžete provádět ručně nebo automaticky. Pro zahájení aktualizace přejděte v [hlavním okně programu](#) na záložku **Aktualizace** a klikněte na možnost **Zkontrolovat aktualizace**.

Po nainstalování programu se standardně vytvoří naplánovaná úloha, která spouští automatickou aktualizaci každou hodinu. Pro změnu délky nastaveného intervalu klikněte na **Nástroje** > [Plánovač](#).

Jak odstranit vir z počítače?

Pokud jeví počítač známky infekce, tzn. je pomalejší, zamrzá apod., doporučujeme postupovat podle následujících kroků:

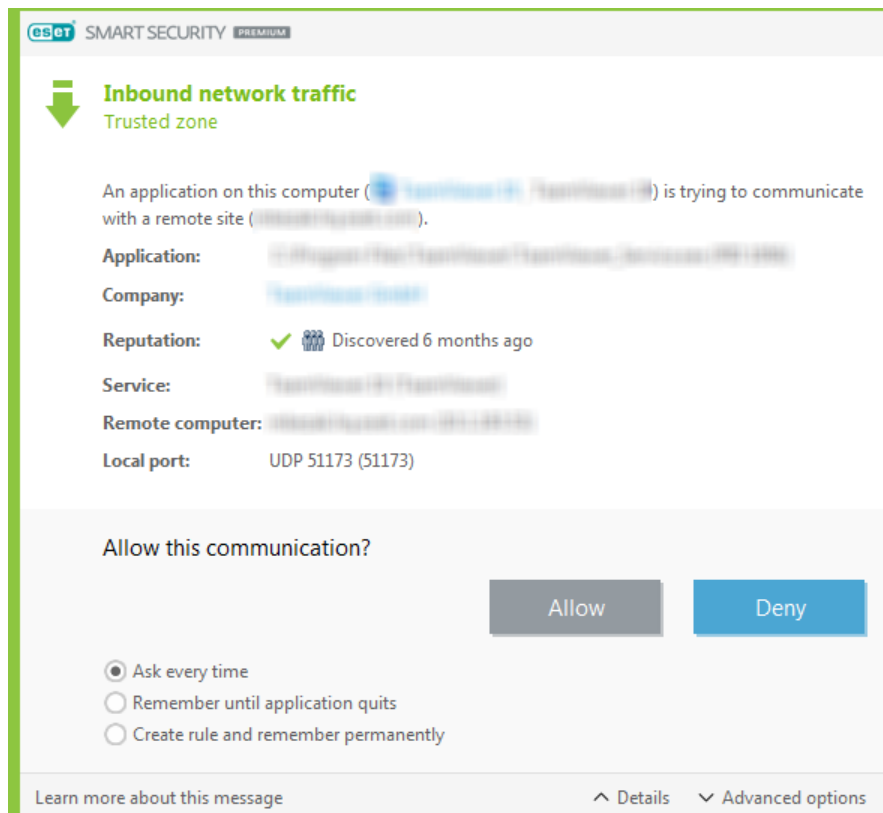
1. V [hlavním okně programu](#) klikněte na záložku **Kontrola počítače**.
2. Klikněte na možnost **Provést kontrolu počítače** pro zahájení jeho kontroly.
3. Po dokončení kontroly si zobrazte její protokol. Zaměřte se především na počet zkontrolovaných, infikovaných a vyléčených souborů.
4. Pokud chcete zkontrolovat pouze vybranou část disku, klikněte na **Volitelná kontrola** a vyberte cíle, které chcete ověřit na přítomnost virů.


Další informace:

- [Článek v ESET Databázi znalostí](#)
- [Karanténa](#)

Jak povolit komunikaci pro konkrétní aplikaci?

Pokud je detekováno nové spojení/komunikace v interaktivním režimu firewallu, pro kterou ještě nebylo vytvořeno pravidlo, zobrazí se dialogové okno, ve kterém můžete komunikaci **Povolit** nebo **Zakázat**. Pokud chcete, aby ESET Smart Security Premium provedl vybranou akci při každém pokusu o komunikaci, zaškrtněte možnost **Zapamatovat akci a vytvořit pravidlo**.



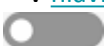
Pro aplikace, které dosud firewall produktu ESET Smart Security Premium nedetekoval, můžete vytvořit nové pravidlo. V [hlavním menu programu](#) klikněte na záložku **Nastavení > Síťová ochrana**. Zde klikněte na ozubené kolečko  na řádku **Firewall** > ze zobrazeného kontextového menu vyberte možnost **Nastavit... > Rozšířené** a na řádku **Pravidla** klikněte na **Změnit**.

Klikněte na tlačítko **Přidat** a na záložce **Obecné** zadejte název pravidla, směr a komunikační protokol pro nové pravidlo. V tomto okně můžete definovat akci, která se provede při aplikaci daného pravidla.

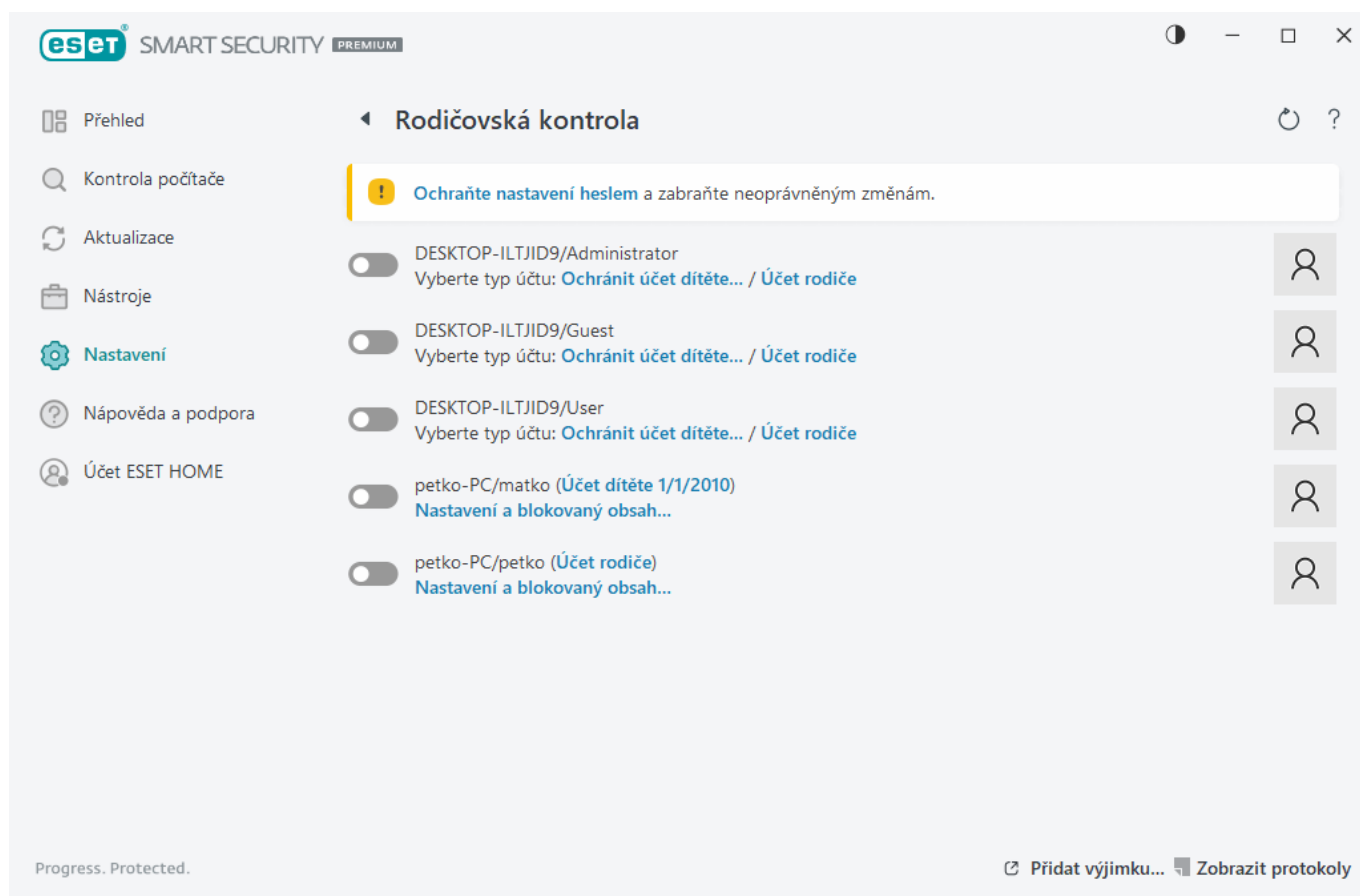
Na záložce **Lokální strana** vyberte aplikaci na tomto počítači, která komunikuje a definujte port. Na záložce **Vzdálená strana** zadejte vzdálenou adresu a port (pokud je to potřeba). Nově vytvořené pravidlo se aplikuje ihned po detekci dané komunikace.

Jak zapnout rodičovskou kontrolu?

K aktivaci Rodičovské kontroly ve vybraném uživatelském účtu postupujte dle následujících kroků:

1. Ve výchozím nastavení ESET Smart Security Premium je Rodičovská kontrola vypnuta. Zapnout ji můžete dvěma způsoby:
 - V [hlavním okně programu](#) přejděte na záložku **Nastavení > Internetová ochrana** a pomocí přepínače  aktivujte **Rodičovskou kontrolu**.
 - Otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana přístupu na web** > **Rodičovská kontrola** a poté pomocí přepínače **zapněte rodičovskou kontrolu**.
2. V [hlavním okně programu](#) přejděte na záložku **Nastavení > Bezpečnostní nástroje > Rodičovská kontrola**. Přestože je funkce **Rodičovské kontroly zapnuta**, je nutné definovat uživatelské účty, pro které se má použít. Klikněte na symbol šipky a dále na možnost **Ochránit účet dítěte**. V následujícím okně vyberte věk, který

odpovídá danému uživateli, podle něhož se stanovuje úroveň filtrování webových stránek. Nyní bude rodičovská kontrola pro vybraný uživatelský účet kompletně nastavená a zapnutá. Dále klikněte na možnost **Nastavení a blokový obsah...** pod jménem účtu k úpravě kategorií, které chcete povolit nebo blokovat v tabulce [Kategorií](#). Pro blokování nebo povolení konkrétních stránek přejděte na záložku [Výjimky](#).



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 kliknutí 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 naplánování úlohy postupujte následovně:

1. Klikněte na tlačítko **Přidat** v hlavním okně Plánovače.
2. Zadejte název úlohy a z rozbalovací nabídky **Typ úlohy** vyberte možnost **Volitelná kontrola počítače**.
3. Vyberte 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 obnovit přístup do heslem chráněných rozšířených nastavení?

Pokud chcete přejít do chráněného zobrazení Rozšířených nastavení, zobrazí se okno pro zadání hesla. Pokud zapomenete nebo ztratíte heslo, klikněte na možnost **Obnovit heslo** a zadejte e-mailovou adresu, kterou jste použili při registraci předplatného. Na tuto adresu vám zašleme ověřovací kód. Daný kód zadejte do zobrazeného dialogového pole a nastavte si nové heslo. Ověřovací kód je platný 7 dní.

Obnovit heslo pomocí účtu ESET HOME – tuto možnost použijte, pokud je předplatné použité k aktivaci spojeno s vaším účtem ESET HOME. Zadejte e-mailovou adresu, kterou se k účtu [ESET HOME](#) přihlašujete.

V případě, že si nepamatujete e-mailovou adresu nebo máte potíže s obnovou hesla, klikněte na možnost **Kontaktovat Technickou podporu**. Následně budete přesměrováni na webový formulář pro kontaktování technické podpory.

Vygenerovat kód pro technickou podporu – pomocí této možnosti vygenerujete kód pro specialistům technické podpory. Následně vyberte možnost **Mám ověřovací kód** a do zobrazeného dialogového pole zadejte kód, který jste obdrželi od specialistů technické podpory, a nastavte si nové heslo. Daný kód zadejte do zobrazeného dialogového pole a nastavte si nové heslo. Ověřovací kód je platný 7 dní.

Více informací naleznete v článku ESET databáze znalostí [Obnovení hesla chránícího přístup do nastavení v domácích produktech pro Windows](#) (článek nemusí být dostupný ve všech jazycích).

Jak deaktivovat produkt prostřednictvím portálu ESET HOME?

Produkt není aktivován

Tato chybová zpráva se zobrazí v případě, že vlastník předplatného deaktivoval váš ESET Smart Security Premium z portálu ESET HOME, případně již nesdílí předplatné s vaším účtem ESET HOME. Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET Smart Security Premium.
- Kontaktujte případně vlastníka předplatného s informací, že je váš ESET Smart Security Premium deaktivovaný nebo že s vámi již předplatné nesdílí. Vlastník licence může problém vyřešit prostřednictvím [portálu ESET HOME](#).

Produkt je deaktivovaný, zařízení je odpojené

Tato chybová zpráva se zobrazí v případě, že bylo [zařízení odebráno ze správcovského portálu ESET HOME](#). Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET Smart Security Premium.
- Obraťte se na vlastníka předplatného s informací, že ESET Smart Security Premium byl deaktivován a zařízení bylo odpojeno od ESET HOME.

- Pokud jste vlastníkem předplatného a o těchto změnách nevíte, zkontrolujte si svůj [Informační kanál o aktivitách ESET HOME](#). Pokud jste zaznamenali podezřelou aktivitu, [změňte si heslo pro přístup do účtu ESET HOME](#) a [kontaktujte Technickou podporu ESET](#).

Produkt je deaktivovaný, zařízení je odpojené

Tato chybová zpráva se zobrazí v případě, že bylo [zařízení odebráno ze správcovského portálu ESET HOME](#). Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET Smart Security Premium.
- Obraťte se na vlastníka předplatného s informací, že ESET Smart Security Premium byl deaktivován a zařízení bylo odpojeno od ESET HOME.
- Pokud jste vlastníkem předplatného a o těchto změnách nevíte, zkontrolujte si svůj [Informační kanál o aktivitách ESET HOME](#). Pokud jste zaznamenali podezřelou aktivitu, [změňte si heslo pro přístup do účtu ESET HOME](#) a [kontaktujte Technickou podporu ESET](#).

Produkt není aktivován

Tato chybová zpráva se zobrazí v případě, že vlastník předplatného deaktivoval váš ESET Smart Security Premium z portálu ESET HOME, případně již nesdílí předplatné s vaším účtem ESET HOME. Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET Smart Security Premium.
- Kontaktujte případně vlastníka předplatného s informací, že je váš ESET Smart Security Premium deaktivovaný nebo že s vámi již předplatné nesdílí. Vlastník licence může problém vyřešit prostřednictvím [portálu ESET HOME](#).

0

Program zvyšování spokojenosti zákazníků

Zapojením se do programu zvyšování spokojenosti zákazníků poskytnete společnosti ESET anonymní informace související s používáním našich produktů. Bližší informace o zpracování dat máme popsány v zásadách ochrany osobních údajů.

Váš souhlas

Účast v programu je dobrovolná a vychází z vašeho souhlasu. Po zapojení se do programu je účast pasivní a nevyžaduje z vaší strany žádné další akce. Své rozhodnutí můžete kdykoli změnit a účast v programu zrušit v nastavení produktu. Tím nám zabráníte v dalším zpracování anonymních dat.

Své rozhodnutí můžete kdykoli změnit a účast v programu zrušit v nastavení produktu.

- [Změna nastavení Programu zvyšování spokojenosti zákazníků v produktech pro domácnosti na platformě Windows](#)

Jaké informace sbíráme?

Data o interakci s produktem

Tyto informace nám pomohou zjistit, jak naše produkty používáte. Díky tomu například víme, jaké funkce používáte nejčastěji, jaké uživatelské nastavení měníte, a kolik času v produktu trávíte.

Data o zařízení

Tyto informace sbíráme za účelem, abychom zjistili, kde a na jakých zařízeních naše produkty používáte. Typicky se jedná o model zařízení, zemi, verzi a název operačního systému.

Diagnostická data o chybách

Sbíráme rovněž informace o chybách a pádech produktu. Příklad: jaká chyba se vyskytla a co jí předcházelo.

Proč tyto informace sbíráme?

Tyto anonymní informace nám pomohou vylepšit naše produkty – pro vás, naše uživatele. To nám pomůže vyvíjet relevantní, snadno ovladatelné a co nejméně problémové produkty, jak jen to bude v našich silách.

Kdo tyto informace spravuje?

Společnost ESET, spol. s r. o. je výhradním správcem dat získaných v rámci tohoto Programu. Tyto informace nejsou sdíleny s třetími stranami.

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtete níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBU POUŽITÍM SOFTWARE 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 Software 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 Software

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, zasláný 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 popsán 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 rozděljuje vícerym uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělována. 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 rozdělovány pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerych 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 prodejci 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_home. 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 uživateli 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 Infiltrace, 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 povinni 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, dekompileovat, 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 uživatelům, 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/nebo 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/nebo 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 uvedena na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompileovat, 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 dotčena práva Poskytovatele spojená s porušením této Dohody.

8. Výhrada práv. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělena v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. Víceré jazykové verze, verze pro více operačních systémů, vícené kopie. V případě jestliže Software podporuje vícené 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 všechny 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 nebo 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/nebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/nebo 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 popsány 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. Tato 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 jakýkoliv 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.

DODATEK K DOHODĚ

Posouzení zabezpečení zařízení připojených k síti. Na posouzení zabezpečení zařízení připojených k síti se vztahují následující dodatečná ustanovení:

Software je vybaven funkcí určenou pro ověření zabezpečení lokální sítě Koncového uživatele a zařízení v lokální síti, k čemuž potřebuje získat název sítě a informace o zařízeních připojených do lokální sítě jako je jejich přítomnost, typ, název, IP adresa a MAC adresa zařízení v lokální síti společně s informací o licenci. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Tato funkce může dále nabízet informace týkající se dostupnosti bezpečnostního software určeného pro zabezpečení zařízení v lokální síti.

Ochrana proti zneužití dat Na ochranu proti zneužití dat se vztahují následující dodatečná ustanovení:

Software obsahuje funkci, která zabraňuje ztrátě nebo zneužití důležitých dat v přímé souvislosti s odcizením počítače. Tato funkce je ve výchozím nastavení Softwaru vypnutá. Aby bylo možné tuto funkci aktivovat, je nutné si vytvořit účet ESET HOME, přes který funkce aktivuje sběr dat v případě odcizení počítače. Pokud tuto funkci Softwaru aktivujete, budou data o odcizeném počítači shromažďována a odesílány Poskytovateli (může se jednat o údaje o umístění počítače v síti, údaje o obsahu zobrazovaném na obrazovce počítače, údaje o konfiguraci počítače nebo o data zaznamenaná kamerou připojenou k počítači (dále jen "Data"). Koncový uživatel je oprávněn používat Data získaná touto funkcí a poskytnutá prostřednictvím účtu ESET HOME výhradně k nápravě nepříznivé situace způsobené odcizením počítače. Výhradně pro účely této funkce Poskytovatel zpracuje Data v souladu se Zásadami ochrany osobních údajů a příslušnými právními předpisy. Poskytovatel umožní Koncovému uživateli přístup k Datům po dobu nezbytně nutnou k dosažení účelu, pro který byla data získána. Tato doba nesmí překročit dobu uchovávání stanovenou v Zásadách ochrany osobních údajů. Ochrana proti zneužití dat se bude používat výlučně u počítačů a účtů, ke kterým má Koncový uživatel oprávněný přístup. Jakékoli nezákonné používání bude oznámeno příslušným orgánům. Poskytovatel bude v případě zneužití postupovat v souladu s příslušnými zákony a pomáhat orgánům činným v trestním řízení. Souhlasíte a potvrzujete, že je Vaší zodpovědností zabezpečit heslo pro přístup k účtu ESET HOME, a souhlasíte s tím, že nesmíte předat své heslo žádné třetí straně. Koncový uživatel je odpovědný za jakoukoli aktivitu, při které se používá funkce ochrany proti zneužití dat a účet ESET HOME, bez ohledu na to, zda k provádění takovýchto aktivit měl nebo neměl povolení. Pokud zjistíte, že je zabezpečení účtu ESET HOME ohroženo, neprodleně tuto skutečnost Poskytovateli oznamte. Dodatečná ustanovení na ochranu proti zneužití dat se vztahují výhradně na koncové uživatele produktů ESET Internet Security a ESET Smart Security Premium.

ESET Secure Data. Na produkt ESET Secure Data se vztahují následující dodatečná ustanovení:

1. Definice. V těchto dodatečných ustanoveních k produktu ESET Secure Data mají následující slova odpovídající významy:

- a) "Informace", jakékoli informace nebo data šifrovaná nebo dešifrovaná pomocí softwaru.
- b) „Produkty“, software ESET Secure Data a související dokumentace;
- c) "ESET Secure Data" Software používaný k šifrování a dešifrování elektronických dat;

Všechny odkazy na množné číslo zahrnují i jednotné číslo a všechny odkazy na mužský rod zahrnují ženský a střední rod a naopak. Slova bez konkrétní definice se používají v souladu s definicemi stanovenými v této Smlouvě.

2. Další deklarace pro Koncové uživatele. Berete na vědomí a souhlasíte s tím, že:

- a) Je vaší zodpovědností chránit, udržovat a zálohovat Informace.
- b) Před instalací softwaru ESET Secure Data byste měli na počítači provést úplnou zálohu všech Informací a dat (mimo jiné včetně důležitých informací a dat).
- c) Je nutné udržovat v bezpečí záznamy o všech heslech nebo jiných informacích používaných pro nastavení a používání softwaru ESET Secure Data a musíte si také vytvořit záložní kopie všech šifrovacích klíčů, licenčních kódů, souborů s klíči a dalších generovaných dat na samostatná úložná média.
- d) Jste zodpovědní za používání Produktů. Poskytovatel nenese odpovědnost za případné ztráty, nároky nebo škody vzniklé v důsledku neoprávněného nebo chybného šifrování nebo dešifrování Informací nebo jiných dat bez ohledu na to, kde a jak jsou tyto Informace nebo jiná data uloženy.
- e) Poskytovatel sice přijal veškerá přiměřená opatření k zajištění integrity a zabezpečení softwaru ESET Secure Data, Produkty (nebo kterýkoli z nich) však nesmí být použity v žádné oblasti, která je závislá na zajištění bezpečnosti při poruše nebo je potenciálně nebezpečná, mimo jiné včetně jaderných zařízení, letecké navigace, řídicích nebo komunikačních systémů, zbraňových a obranných systémů, podpůrných zařízení a systémů monitorování životních funkcí.
- f) Je povinností Koncového uživatele zajistit, aby úroveň zabezpečení a šifrování zajišťovaná produkty byla adekvátní vašim požadavkům.
- g) Jste zodpovědní za používání Produktů (nebo kteréhokoli z nich), mimo jiné včetně zajištění toho, aby bylo jejich používání v souladu se všemi platnými zákony a předpisy Slovenské republiky nebo jakékoli jiné země, oblasti nebo státu, kde se Produkty používají. Před každým použitím Produktů musíte zajistit, aby nebylo v rozporu s embargem žádné vlády (Slovenské republiky nebo jiné země/oblasti).
- h) Software ESET Secure Data může čas od času kontaktovat servery Poskytovatele s cílem zkontrolovat informace o licenci a dostupnost oprav, aktualizací Service Pack a dalších aktualizací, které mohou být určeny k vylepšování, údržbě, pozměnění nebo rozšíření softwaru ESET Secure Data a v souladu se Zásadami ochrany osobních údajů může odesílat obecné informace o systému související s funkčností Softwaru.
- i) Poskytovatel nenese odpovědnost za jakékoli ztráty, škody, výdaje nebo nároky vyplývající ze ztráty, odcizení, zneužití, poškození nebo zničení hesel, instalačních informací, šifrovacích klíčů, licenčních aktivačních kódů a dalších dat generovaných nebo uložených během používání softwaru.

Dodatečná ustanovení k produktu ESET Secure Data se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

Software Password Manager. Na software Password Manager se vztahují následující dodatečná ustanovení:

- 1. Další deklarace pro Koncové uživatele. Berete na vědomí a souhlasíte s tím, že nesmíte:

a) Používat software Password Manager k provozování jakékoli aplikace důležité pro chod firmy, kde by mohlo dojít k ohrožení lidských životů nebo k újmě na majetku. Berete na vědomí, že software Password Manager není k takovým účelům určen a že jeho selhání v takových případech by mohlo vést ke smrti, újmám na zdraví či vážným škodám na majetku nebo prostředí, za které Poskytovatel neodpovídá.

SOFTWARE PASSWORD MANAGER NENÍ NAVRŽEN, URČEN ANI LICENCOVÁN K POUŽITÍ V RIZIKOVÝCH PROSTŘEDÍCH VYŽADUJÍCÍCH ZAJIŠTĚNÍ BEZPEČNOSTI PŘI PORUŠE, MIMO JINÉ VČETNĚ NÁVRHU, VÝSTAVBY, ÚDRŽBY NEBO PROVOZU JADERNÝCH ZAŘÍZENÍ, LETECKÝCH NAVIGAČNÍCH NEBO KOMUNIKAČNÍCH SYSTÉMŮ, ŘÍZENÍ LETOVÉHO PROVOZU A SYSTÉMŮ PODPORY ŽIVOTNÍCH FUNKCÍ NEBO ZBRAŇOVÝCH SYSTÉMŮ. POSKYTOVATEL VÝSLOVNĚ ODMÍTÁ JAKÉKOLI VÝSLOVNĚ UVEDENÉ ČI PŘEDPOKLÁDANÉ ZÁRUKY VHODNOSTI PRO TYTO ÚČELY.

b) Používat software Password Manager způsobem, který porušuje podmínky této smlouvy či zákony Slovenské republiky nebo vaší jurisdikce. Konkrétně nesmíte software Password Manager používat k provádění nebo propagování jakékoli nezákonné činnosti, včetně nahrávání dat škodlivého obsahu či obsahu, který by se mohl používat pro jakoukoli nezákonnou činnost, který by mohl jakýmkoli způsobem porušovat zákony nebo práva jakékoli třetí strany (včetně jakýchkoli práv duševního vlastnictví), mimo jiné včetně jakýchkoli pokusů o získání přístupu k účtům v Úložišti (pro účely těchto dodatečných podmínek k softwaru Password Manager termín Úložiště označuje prostor pro ukládání dat spravovaných Poskytovatelem nebo třetí stranou, která není Poskytovatelem, a uživatelem pro účely umožnění synchronizace a zálohování uživatelských dat) nebo k jakýmkoli účtům a datům jiných uživatelů softwaru Password Manager nebo uživatelů Úložiště. Pokud porušíte kterékoli z těchto ustanovení, je Poskytovatel oprávněn okamžitě ukončit platnost této smlouvy a požadovat od vás náhradu ve výši nákladů na nezbytnou nápravu, jakož i učinit všechny nezbytné kroky k tomu, aby vám zabránil v dalším používání softwaru Password Manager bez možnosti náhrady.

2. OMEZENÍ ODPOVĚDNOSTI. SOFTWARE PASSWORD MANAGER JE POSKYTOVÁN "TAK JAK JE", BEZ ZÁRUKY JAKÉHOKOLIV DRUHU, AŽ UŽ VÝSLOVNĚ VYJÁDŘENÉ NEBO PŘEDPOKLÁDANÉ. SOFTWARE POUŽÍVÁTE NA VLASTNÍ NEBEZPEČÍ. VÝROBCE NEODPOVÍDÁ ZA ZTRÁTU DAT, ŠKODY, OMEZENÍ DOSTUPNOSTI SLUŽEB, VČETNĚ JAKÝCHKOLI DAT ODESLANÝCH SOFTWAREM PASSWORD MANAGER DO EXTERNÍHO ÚLOŽIŠTĚ PRO ÚČELY SYNCHRONIZACE A ZÁLOHOVÁNÍ DAT. ŠIFROVÁNÍ DAT POMOCÍ SOFTWARE PASSWORD MANAGER NEZAKLÁDÁ ŽÁDNOU ODPOVĚDNOST POSKYTOVATELE S OHLEDEM NA ZABEZPEČENÍ TĚCHTO DAT. VÝSLOVNĚ SOUHLASÍTE S TÍM, ŽE DATA ZÍSKANÁ, POUŽÍVANÁ, ŠIFROVANÁ, UKLÁDANÁ, SYNCHRONIZOVANÁ NEBO ODESÍLANÁ POMOCÍ SOFTWARE PASSWORD MANAGER JE TAKÉ MOŽNÉ UKLÁDAT NA SERVERY TŘETÍCH STRAN (VZTAHUJE SE POUZE NA TAKOVÉ POUŽÍVÁNÍ SOFTWARE PASSWORD MANAGER, KDE BYLY POVOLENY SLUŽBY SYNCHRONIZACE A ZÁLOHOVÁNÍ). POKUD SE POSKYTOVATEL DLE SVÉHO VLASTNÍHO UVÁŽENÍ ROZHODNE POUŽÍVAT TAKOVÉ ÚLOŽIŠTĚ, WEB, WEBOVÝ PORTÁL, SERVER NEBO SLUŽBU TŘETÍ STRANY, NENESE POSKYTOVATEL ODPOVĚDNOST ZA KVALITU, BEZPEČNOST ČI DOSTUPNOST TAKOVÉ SLUŽBY TŘETÍ STRANY, PŘIČEMŽ POSKYTOVATEL VŮČI VÁM NEMÁ ŽÁDNOU ODPOVĚDNOST ZA PORUŠENÍ SMLUVNÍCH NEBO ZÁKONNÝCH POVINNOSTÍ TŘETÍ STRANOU ANI ZA ŠKODY, UŠLÝ ZISK, FINANČNÍ NEBO NEFINANČNÍ ŠKODY NEBO JAKÝKOLI JINÝ DRUH ZTRÁTY PŘI POUŽÍVÁNÍ TOHOTO SOFTWARE. POSKYTOVATEL NENÍ ZODPOVĚDNÝ ZA OBSAH ŽÁDNÝCH DAT ZÍSKANÝCH, POUŽÍVANÝCH, ŠIFROVANÝCH, UKLÁDANÝCH, SYNCHRONIZOVANÝCH NEBO ODESÍLANÝCH POMOCÍ SOFTWARE PASSWORD MANAGER NEBO V ÚLOŽIŠTI. BERETE NA VĚDOMÍ, ŽE POSKYTOVATEL NEMÁ PŘÍSTUP K OBSAHU ULOŽENÝCH DAT A NENÍ SCHOPEN MONITOROVAT NEBO ODSTRAŇOVAT PRÁVNĚ ZÁVADNÝ OBSAH.

Poskytovatel vlastní všechna práva na vylepšení, upgrady a opravy související se softwarem Password Manager ("Vylepšení"), a to i v případě, že kterákoli z těchto vylepšení byla vytvořena na základě názorů, nápadů nebo návrhů předložených vámi, a to v jakémkoliv formě. Nebudete mít nárok na žádnou náhradu škody, mimo jiné včetně jakýchkoli licenčních poplatků souvisejících s takovými Vylepšeními.

SUBJEKTY POSKYTOVATELE A VLASTNÍCI LICENCÍ NEBUDOU MÍT VŮČI VÁM ŽÁDNOU ZODPOVĚDNOST ZA POHLEDÁVKY A ZÁVAZKY JAKÉHOKOLIV DRUHU VZNIKLE Z NEBO SE JAKÝMKOLI ZPŮSOBEM TÝKAJÍCÍ POUŽÍVÁNÍ SOFTWARE PASSWORD MANAGER VÁMI NEBO TŘETÍMI STRANAMI, POUŽITÍ NEBO NEPOUŽITÍ JAKÉKOLI

ZPROSTŘEDKOVATELSKÉ SPOLEČNOSTI ČI PRODEJCE NEBO PRODEJE ČI NÁKUPU JAKÝCHKOLI CENNÝCH PAPIRŮ BEZ OHLEDU NA TO, ZDA TAKOVÉ POHLEDÁVKY A ZÁVAZKY VYCHÁZEJÍ Z NĚJAKÉ ZÁKONNÉ NEBO SPRÁVEDLIVÉ TEORIE.

SUBJEKTY POSKYTOVATELY A VLASTNÍCI LICENCÍ NEBUDOU MÍT VŮČI VÁM ŽÁDNOU ZODPOVĚDNOST ZA ŽÁDNÉ PŘÍMÉ, NAHODILÉ, ZVLÁŠTNÍ, NEPŘÍMÉ NEBO NÁSLEDNÉ ŠKODY VYPLÝVAJÍCÍ Z NEBO VE SPOJENÍ S JAKÝMKOLI SOFTWAREM TŘETÍCH STRAN, JAKÝMKOLI DATY VYUŽÍVANÝMI PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, VAŠE POUŽÍVÁNÍ NEBO NESCHOPNOST POUŽÍVAT SOFTWARE PASSWORD MANAGER (NEBO K NĚMU ZÍSKAT PŘÍSTUP) NEBO JAKÝMKOLI DATY POSKYTOVANÝMI PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, AŽ JIŽ JSOU TAKOVÁ ODŠKODNĚNÍ NÁROKOVÁNA NA ZÁKLADĚ JAKÉKOLI ZÁKONNÉ NEBO SPRÁVEDLIVÉ TEORIE. ŠKODY VYLOUČENÉ TOUTO KLAUZULÍ ZAHRNÚJÍ MIMO JINÉ ŠKODY ZPŮSOBENÉ ZTRÁTOU ZISKU, ÚJMOU NA ZDRAVÍ NEBO NA MAJETKU, PŘERUŠENÍ PODNIKATELSKÉ ČINNOSTI NEBO ZTRÁTOU OBCHODNÍCH ČI OSOBNÍCH ÚDAJŮ. NĚKTERÉ JURISDIKCE NEUMOŽŇUJÍ OMEZENÍ NAHODILÝCH NEBO NÁSLEDNÝCH ŠKOD. V TAKOVÝCH PŘÍPADECH SE NA VÁS TOTO OMEZENÍ NEMUSÍ VZTAHOVAT. V TAKOVÉM PŘÍPADĚ BUDE ZODPOVĚDNOST POSKYTOVATELE V MINIMÁLNÍM ROZSAHU POVOLENÉM PLATNÝMI ZÁKONY.

INFORMACE POSKYTNUTÉ PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, VČETNĚ CEN AKCIÍ, ANALÝZ, INFORMACÍ O TRHU, ZPRÁV A FINANČNÍCH DAT, MOHOU BÝT ZPOŽDĚNY, NEPŘESNÉ NEBO MOHOU OBSAHOVAT CHYBY NEBO OPOMENUTÍ A SUBJEKTY POSKYTOVATELE A VLASTNÍCI LICENCÍ NENESOU V SOUVISLOSTI S NIMI ŽÁDNOU ODPOVĚDNOST. POSKYTOVATEL MŮŽE ZMĚNIT NEBO PŘESTAT NABÍZET VEŠKERÉ ASPEKTY NEBO FUNKCE SOFTWARE PASSWORD MANAGER NEBO POUŽÍVÁNÍ VŠECH NEBO NĚKTERÝCH FUNKCÍ NEBO TECHNOLOGIÍ V SOFTWARE PASSWORD MANAGER, A TO KDYKOLI BEZ PŘEDCHOZÍHO OZNÁMENÍ.

POKUD JSOU USTANOVENÍ V TOMTO ČLÁNKU Z JAKÉHOKOLIV DŮVODU NEPLATNÁ NEBO POKUD JE POSKYTOVATEL POVAŽOVÁN ZA ODPOVĚDNÉHO ZA ŠKODY ATD. PODLE PLATNÝCH ZÁKONŮ, STRANY SE DOHODLY, ŽE ODPOVĚDNOST POSKYTOVATELE VŮČI VÁM BUDE OMEZENA NA CELKOVOU ČÁSTKU LICENČNÍCH POPLATKŮ, KTERÉ JSTE ZAPLATILI.

SOUHLASÍTE S TÍM, ŽE ODŠKODNÍTE A BUDETE CHRÁNIT A BRÁNIT POSKYTOVATELE A JEHO ZAMĚŠTNANCE, DCEŘINÉ SPOLEČNOSTI, AFILACE, PARTNERY Z OBLASTI REBRANDINGU A DALŠÍ PARTNERY PŘED JAKÝMKOLI A VŠEMI POHLEDÁVKAMI, ZÁVAZKY, ŠKODAMI, ZTRÁTAMI, NÁKLADY, VÝDAJI A POPLATKY TŘETÍCH STRAN (MIMO JINÉ VČETNĚ VLASTNÍKŮ ZAŘÍZENÍ NEBO STRAN, JEJICHŽ PRÁVA BYLA OVLIVNĚNA DATY POUŽITÝMI V SOFTWARE PASSWORD MANAGER NEBO V ÚLOŽIŠTI).

3. Data v softwaru Password Manager. Pokud výslovně nezvolíte jiné nastavení, budou všechna data zadaná vámi, která budou uložena v databázi softwaru Password Manager, uložena v zašifrované podobě na počítači nebo jiném paměťovém zařízení, které definujete. Berete na vědomí, že v případě odstranění nebo poškození jakýchkoli databázových nebo jiných souborů softwaru Password Manager budou všechna data v nich obsažená nenávratně ztracena, přičemž chápete a akceptujete riziko takové ztráty. Skutečnost, že se vaše osobní data ukládají na počítači v zašifrované podobě, neznamená, že tyto informace nemohou být odcizeny nebo zneužity někým, kdo objeví hlavní heslo nebo získá přístup k aktivnímu zařízení definovanému zákazníkem pro otevření databáze. Jste zodpovědní za udržování bezpečnosti všech způsobů přístupu.

4. Odesílání osobních údajů Poskytovateli nebo do Úložiště. Pokud se tak rozhodnete (a výhradně za účelem zajištění včasné synchronizace a zálohování dat), bude software Password Manager přenášet nebo odesílat osobní údaje z databáze softwaru Password Manager (konkrétně hesla, přihlašovací údaje, informace o účtech a identitách) přes internet do Úložiště. Data jsou přenášena výhradně v šifrované podobě. Použití softwaru Password Manager pro vyplňování hesel, přihlašovacích údajů či jiných údajů do online formulářů může vyžadovat, aby byly informace odesílány přes internet na weby, které určíte. Tento přenos dat není iniciován softwarem Password Manager, Poskytovatel proto nemůže být zodpovědný za bezpečnost takových interakcí s jakýmkoli weby podporovanými různými poskytovateli. Veškeré transakce probíhající přes internet (bez ohledu na to, zda ve spojení se softwarem Password Manager) jsou na vašem vlastním uvážení a na vaše vlastní riziko a budete mít výhradní odpovědnost za jakékoli poškození vašeho počítačového systému nebo ztrátu dat vyplývající

ze stažení a/nebo používání takovýchto materiálů nebo služeb. Aby se minimalizovalo riziko ztráty cenných dat, doporučuje Poskytovatel, aby Koncoví uživatelé prováděli pravidelné zálohy databáze a dalších citlivých souborů na externí disky. Poskytovatel vám není schopen nijak pomoci s obnovením ztracených nebo poškozených dat. Pokud Poskytovatel poskytuje služby zálohování k uživatelským databázovým souborům pro případ poškození nebo odstranění souborů na počítačích uživatelů, je taková služba zálohování poskytována bez jakékoli záruky a neimplikuje žádnou odpovědnost Poskytovatele vůči vám.

Používáním softwaru Password Manager souhlasíte s tím, že software může čas od času kontaktovat servery Poskytovatele s cílem zkontrolovat informace o licenci a dostupnost oprav, aktualizací Service Pack a dalších aktualizací, které mohou být určeny k vylepšování, údržbě, pozměnění nebo rozšíření softwaru Password Manager. Software může odesílat obecné systémové informace týkající se fungování softwaru Password Manager v souladu se Zásadami ochrany osobních údajů.

5. Informace a pokyny k odinstalaci. Veškeré informace z databáze, které byste chtěli zachovat, si musíte před odinstalací softwaru Password Manager vyexportovat.

Dodatečná ustanovení k softwaru Password Manager se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

ESET LiveGuard. Na produkt ESET LiveGuard se vztahují následující dodatečná ustanovení:

Software obsahuje funkci další analýzy souborů odeslaných Koncovým uživatelem. Poskytovatel bude soubory odeslané Koncovým uživatelem a výsledky analýzy používat pouze v souladu se Zásadami ochrany osobních údajů a v souladu s příslušnými právními předpisy.

Dodatečná ustanovení k produktu ESET LiveGuard se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Zásady ochrany osobních údajů

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvláště důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Právní základ pro zpracování osobních údajů

Při zpracování dat používáme v souladu s příslušným legislativním rámcem v souvislosti s ochranou osobních údajů jen několik právních základů. Zpracování osobních údajů ve společnosti ESET je potřebné zejména za účelem plnění dokumentu [Licenční ujednání s koncovým uživatelem](#) („EULA“) odsouhlaseného s koncovým uživatelem (dle článku 6 (1) (b) nařízení GDPR), který je platný pro poskytování produktů nebo služeb společnosti ESET, pokud není výslovně uvedeno jinak, například:

- Oprávněný zájem: Právní základ (dle článku 6 (1) (f) nařízení GDPR), který nám umožňuje zpracovávat údaje o tom, jak naši zákazníci využívají naše služby a jak jsou s nimi spokojeni, abychom jim mohli poskytnout nejlepší možnou ochranu, podporu a služby. Podle platných právních předpisů je za oprávněný zájem považován i marketing, proto se při marketingové komunikaci s našimi zákazníky obvykle spoléháme na tento koncept.
- Souhlas (dle článku 6 (1) (a) nařízení GDPR): Můžeme jej od vás vyžadovat v konkrétních situacích, kdy považujeme tento právní základ za nejvhodnější, nebo pokud to vyžaduje zákon.
- Splnění zákonné povinnosti (dle článku 6 (1) (c) nařízení GDPR): Například specifikace požadavků na elektronickou komunikaci nebo uchovávání dokumentů souvisejících s fakturací.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodeje, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Zabezpečení dat

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 příslušné dozorčí orgány i ohrožené koncové uživatele jakožto subjekty údajů.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a –

pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úřad na ochranu osobních údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v dokumentu [Licenční ujednání s koncovým uživatelem](#), 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 v Licenčním ujednání s koncovým uživatelem („EULA“) a v produktové [dokumentaci](#). Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

Licenční a fakturační údaje. Jméno, e-mailová adresa, licenční klíč a (v některých případech) adresa, afilace společnosti a platební údaje jsou společností ESET shromažďovány a zpracovávány za účely aktivace licence, doručení licenčního klíče, připomenutí konce platnosti, požadavků na podporu, ověření pravosti licence, poskytování našich služeb a dalších oznámení, včetně marketingových zpráv v souladu s příslušnými zákony nebo vašim souhlasem. Společnost ESET má zákonnou povinnost uchovávat fakturační údaje po dobu 10 let, ovšem informace o licencích jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

Aktualizace a další statistiky. Mezi zpracovávané informace patří 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, adresa MAC a nastavení konfigurace produktu. Tyto informace jsou zpracovávány za účelem poskytování služeb aktualizace a upgradu a za účelem údržby, zabezpečení a vylepšování naší backendové infrastruktury.

Tyto informace jsou uchovávány odděleně od identifikačních údajů potřebných pro účely licencování a fakturace, protože nevyžadují identifikaci koncového uživatele. Doba uchovávání je maximálně 4 roky.

Reputační systém **ESET LiveGrid®**. Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jsou zpracovávány pro účely reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu. Koncový uživatel během tohoto procesu není identifikován.

Systém zpětné vazby **ESET LiveGrid®**. 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 týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
- Soubory výpisu chyb a v nich obsažené informace.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. 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.

Veškeré informace získané a zpracovávané prostřednictvím systému zpětné vazby ESET LiveGrid® jsou určeny k použití bez identifikace koncového uživatele.

Posouzení zabezpečení zařízení připojených k síti. Abychom mohli poskytovat funkci posouzení zabezpečení,

zpracováváme název lokální sítě a informace o zařízeních v lokální síti, jako jsou přítomnost, typ, název, IP adresa a adresa MAC zařízení v lokální síti společně s informacemi o licencích. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Informace o licencích identifikující koncové uživatele jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

Technická podpora. Za účelem poskytování podpory mohou být vyžadovány kontaktní a licenční informace a údaje obsažené ve vašich požadavcích na podporu. 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. Údaje zpracováváné za účelem poskytování technické podpory jsou ukládány na dobu 4 let.

Ochrana proti zneužití dat Pokud koncový uživatel vytvoří účet ESET HOME na webu <https://home.eset.com> a aktivuje tuto funkci v souvislosti s krádeží počítače, budou shromážděny a zpracovány následující informace: údaje o poloze, snímky obrazovky, data o konfiguraci počítače a data zaznamenaná kamerou počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb a jsou uchovávány po dobu 3 měsíců.

Password Manager. Pokud se rozhodnete aktivovat funkci Password Manager, budou data související s vašimi přihlašovacími údaji uložena v šifrované podobě pouze na vašem počítači nebo jiném určeném zařízení. Pokud aktivujete synchronizační službu, šifrované údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb, abychom tuto službu mohli zajistit. Společnost ESET ani poskytovatelé služeb nemají k šifrovaným datům přístup. Pouze Vy máte klíč potřebný k dešifrování dat. Tato data budou odebrána při deaktivaci této funkce.

ESET LiveGuard. Pokud se rozhodnete aktivovat funkci ESET LiveGuard, bude třeba odesílat vzorky, jako jsou soubory předdefinované a vybrané koncovým uživatelem. Vzorky, které vyberete ke vzdálené analýze, budou odeslány do služby společnosti ESET a výsledky analýzy budou odeslány zpět do vašeho počítače. Veškeré podezřelé vzorky se zpracovávají stejným způsobem jako informace shromážděné systémem zpětné vazby ESET LiveGrid®.

Program zvyšování spokojenosti zákazníků Pokud jste se rozhodli aktivovat [Program zvyšování spokojenosti zákazníků](#), budou na základě Vašeho souhlasu shromažďovány a používány anonymní telemetrické informace týkající se používání našich produktů.

Upozorňujeme, že pokud osoba používající naše produkty a služby není koncový uživatel, který si zakoupil produkt nebo službu a uzavřel s námi smlouvu EULA (například zaměstnanec koncového uživatele, člen rodiny nebo osoba, která od koncového uživatele jiným způsobem dostala oprávnění používat produkt nebo službu v souladu se smlouvou EULA), je zpracování údajů prováděno na základě oprávněného zájmu společnosti ESET, jak je definován v článku 6 (1) f) nařízení GDPR, abychom mohli uživateli autorizovanému koncovým uživatelem umožnit používání námi poskytovaných produktů a služeb v souladu se smlouvou EULA.

Kontaktní informace

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.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk